日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年１０月２４日

出願番号
Application Number: 特願２００１－３２６９０８

出願人
Applicant(s): 宇山　靖政

２００１年１２月２１日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願
【整理番号】　1119
【特記事項】　特許法第３０条第１項の規定の適用を受けようとする特許出願
【あて先】　特許庁長官殿
【国際特許分類】　H04K　1/00
【発明者】
　【住所又は居所】　神奈川県横須賀市久里浜八丁目３０番１５号５０４
　【氏名】　宇山　靖政
【特許出願人】
　【識別番号】　300085864
　【氏名又は名称】　宇山　靖政
【代理人】
　【識別番号】　100098899
　【弁理士】
　【氏名又は名称】　飯塚　信市
【先の出願に基づく優先権主張】
　【出願番号】　特願2000-388921
　【出願日】　平成12年12月21日
【手数料の表示】
　【予納台帳番号】　037486
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0113776
【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　秘密通信方法

【特許請求の範囲】

【請求項１】　記憶装置と演算装置を利用できる情報機器による暗号を利用した秘密通信の方法のうちで、送信者と受信者の順序対に対して一意的に決まる暗号化方式と復号化方式に従って暗号を利用した通信を自動的に行うもので、順序対に対応する暗号化方式を受信者が前もって自由に指定しておくことができる秘密通信の方法。

【請求項２】　暗号化の指定欄と復号化の指定欄がある識別記号一覧を備え、送信時には情報の受信者が前もって指定した方式により自動的に暗号化を行い、受信時には送信者に対応する復号化方式により自動的に復号化することで、請求項１の秘密通信の方法を実現する秘密通信用ソフトウェア。

【請求項３】　暗号ソフトの形式のうち、暗号化部分と復号化部分に分割でき、暗号化部分の自由な再配布を認めるが、復号化部分の自由な再配布は認めない形式。

【請求項４】　有料での情報配信の方法で、上記の請求項１，２，３の利用によって少なくとも顧客の要求する以上の強度を持つ暗号化によって情報を配信する方法。

【請求項５】　ネットワークを通じた通信機能を有するパーソナルコンピュータ等の情報処理装置に適用される秘密通信用ソフトウェアであって、

送信予定ファイルについての所定の暗号化指示入力があったときには、そのとき指定された送信先データと、送信先データと使用暗号化プログラムとが予め対応づけられた参照テーブルとに基づき、前記情報処理装置の有する記憶手段に予め記憶された複数種の暗号化プログラムから使用すべき暗号化プログラムを自動特定し、当該暗号化プログラムにしたがって、前記送信予定ファイルを自動暗号化する機能と、

受信済み暗号化ファイルについての所定の復号化指示入力があったときには、当該暗号化ファイルの送信元データと、送信元データと使用復号化プログラムとが予め対応付けられた参照テーブルとに基づき、記憶手段に記憶された複数種の

複合化プログラムから使用すべき複合化プログラムを自動特定し、当該復号化プログラムにより前記受信済み暗号化ファイルを自動復号化する機能と、

を具備する秘密通信用ソフトウェア。

【請求項６】　参照テーブルとして情報処理装置に別途記憶されている電子メールソフトのアドレス帳機能を利用するとともに、自動暗号化された送信予定ファイルを当該電子メールソフトによる電子メールに添付してそのとき指定された送信先へと自動送信するための電子メールソフト互換機能を有する、ことを特徴とする請求項５に記載の秘密通信用ソフトウェア。

【請求項７】　参照テーブルにおいては、１つの送信先データに対して複数種の暗号化プログラムが適用順データとともに対応づけ可能とされており、当該対応付けがなされている送信先データで特定される送信予定ファイルは、それら複数種の暗号化プログラムを適用順データに基づき順番に使用することにより多重暗号化され、

また、参照テーブルにおいては、１つの送信元データに対して複数種の復号化プログラムが対応付け可能とされており、当該対応付けがなされている送信元データで特定される復号化ファイルは、それら複数種の復号化プログラムを適用順データに基づき順番に使用することにより復号化が行われる、ことを特徴とする請求項５又は６に記載の秘密通信用ソフトウェア。

【請求項８】　参照テーブルには、各送信先データまたは送信元データ毎に、電子メール本文と電子メール添付ファイルとのそれぞれについて別個に複数の暗号化プログラムまたは復号化プログラムを対応付け可能とされている、ことを特徴とする請求項７に記載の秘密通信用ソフトウェア。

【請求項９】　適用順データは、予め定められた規則に基づき適宜自動変更される、ことを特徴とする請求項７または８に記載の秘密通信用ソフトウェア。

【請求項１０】　ナンバーディスプレイ等の発信者通知機能を有する電話機であって、

暗号化プログラムおよび復号化プログラムとを入力する手段と、

発信先データと任意の暗号化プログラムとを対応づけて暗号化参照データとして予め記憶させるための手段と、

発信元データと任意の複合化プログラムとを対応づけて復号化参照データとして予め記憶させるための記憶手段と、

そのときの通話に係る発信先データと前記暗号化参照データとに基づきその通話に際して使用する暗号化プログラムを特定し、当該暗号化プログラムを使用して送信すべき音声信号を適宜暗号化して送信する手段と、

そのときの通話に係る発信者データと前記復号化参照データとに基づきそのとき使用する複合化プログラムを特定し、当該復号化プログラムを使用して順次受信される音声信号を適宜複合化して音声出力する手段と、

を有する、電話機。

【請求項１１】　参照テーブルにおいては、１つの発信先データに対して複数種の暗号化プログラムが対応づけ可能とされており、当該対応付けがなされている発信先への送信される音声信号は、それら複数種の暗号化プログラムに基づき多重暗号化され、

また、参照テーブルにおいては、１つの発信元データに対して複数種の復号化プログラムが対応付け可能とされており、当該対応付けがなされている発信元から送信されてくる音声信号は、それら複数種の復号化プログラムに基づき多重復号化される、ことを特徴とする請求項１０に記載の電話機。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、ネットワークを利用した秘密通信方法に係り、特に、送信先毎に定められた暗号化方式により送信すべきファイル等を自動暗号化することにより、通信傍受等を防止した安全性の高い通信を簡易に実現可能とした秘密通信方法に関する。

【０００２】

【従来の技術】

昨今のＩＴ革命に伴い、例えば電子メール等によるインターネット通信は現代社会に欠かすことができないものとなりつつあるが、一方で、そのようなインターネット通信にあっては、通信傍受の被害が後を絶たず、その安全性、信頼性が

問題視されている。図１６は通信傍受の手口の一例を示すものであり、同図には、スニッファと呼ばれる傍受装置をネットワーク上（この例ではルータの入り口付近）に無断で仕掛け、非合法にパスワード等の重要情報を傍受する場合が示されている。

【０００３】

【発明が解決しようとする課題】

このような通信傍受を防ぐ一対策として暗号化通信の採用が考えられる。しかしながら、現状、暗号化通信の利用に際しては面倒な準備や高い費用が必要とされることから、一般には普及されておらず、仮に、暗号化通信方式を採用した場合にも、その方式は固定されたものとなりがちであり、解読がされやすく、依然として通信傍受に対する安全性が確保され難いものであった。

【０００４】

この発明は、上述の問題点に着目してなされたものであり、その目的とするところは、ネットワークを通じたより安全性の高い通信を行うための秘密通信方法を提供することにある。

【０００５】

この発明の他の目的とするところは、ネットワーク上での安全性の高い秘密通信を実現するためのコンピュータソフトウェアを提供することにある。

【０００６】

この発明の更に他の目的とするところは、そのような秘密通信方法の普及を通じて、安全で信頼性のあるネットワーク社会の実現を図ることにある。

【０００７】

この発明のさらに他の目的乃至作用効果については、以下の明細書の記載を参照することにより、当業者であれば容易に理解されるであろう。

【０００８】

【課題を解決するための手段】

本発明の第１実施形態は、記憶装置と演算装置を利用できる情報機器による暗号を利用した秘密通信方法として実現される。送信するデータは、送信者と受信者の順序対に対して一意的に決まる暗号化方式に従って自動的に暗号化される。

暗号化されたデータは、引き続き自動送信されるようにすると好ましい。

【０００９】

尚、ここでは、原則として順序対に対応する暗号化方式を受信者が前もって自由に指定しておくようにする。これは、暗号化されたデータの復号化が受信者側で有する復号化方式に完全に依存されるためであり当然のことと思われるが、あくまでも原則であり、‘決定権’を必ずしも受信者側に与える必要もないであろう。

【００１０】

このようにして暗号化されたデータは、同様に、受信者の側において、送信者と受信者の順序対に対して一意的に決まる復号化方式に従ってって自動的に復号化される。

【００１１】

本発明の第２実施形態は、上記第１実施形態の秘密通信をコンピュータ端末機を使用して実現するための秘密通信用ソフトウェアとして実現される。この通信用ソフトウェアは、暗号化方式の指定欄と復号化方式の指定欄があるアドレス帳機能（識別記号記憶・一覧表示機能）を備える。データの送信時には、暗号化方式の指定欄により特定される方式により自動的に暗号化が行われる。受信時には、復号化方式の指定欄で特定される方式により自動的に暗号化されたファイル等の復号化が行われる。

【００１２】

尚、暗号化方式、復号化方式とあるが、これらは、使用される暗号化鍵、暗号化ソフト、復号化鍵、復号化ソフト等に基づき特定される。尚、各方式をそのような暗号化ソフト、復号化ソフトに基づき実現するような場合、それらは、予めこの通信用ソフトウェアに組み込んでおいてもよいが、別途、更新乃至入力するようにしておけば、方式の変更、入れ替え等も容易となる。

【００１３】

好ましくは、第２実施形態の秘密通信用ソフトウェアは、暗号化鍵・暗号化ソフト等の暗号化部分と復号化鍵・復号化ソフト等の復号化部分とを含んでなり、暗号化部分については自由な再配布が認められるが、復号化部分の自由な再配布

は認めないようにする。

【００１４】

このようにすることで、秘密通信用ソフトウェアを商業ベースで開発販売することを経済的に保証でき、優れた通信用ソフトウェアが安定して供給される。

【００１５】

上記第１実施形態または第２実施形態を有料での情報配信に適用するような場合には、少なくとも顧客の要求する以上の強度を持つ暗号化によって情報を配信するようにするのが好ましい。尚、「強度」は、例えば、多重暗号化により確保することができる。

【００１６】

本発明の第３実施形態は、ネットワークを通じた通信機能を有するパーソナルコンピュータ等の情報処理装置に適用される秘密通信用ソフトウェアであって、送信予定ファイルについての所定の暗号化指示入力があったときには、そのとき指定された送信先データと、送信先データと使用暗号化プログラムとが予め対応づけられた参照テーブルとに基づき、前記情報処理装置の有する記憶手段に予め記憶された複数種の暗号化プログラムから使用すべき暗号化プログラムを自動特定し、当該暗号化プログラムにしたがって、前記送信予定ファイルを自動暗号化する機能と、受信済み暗号化ファイルについての所定の復号化指示入力があったときには、当該暗号化ファイルの送信元データと、送信元データと使用復号化プログラムとが予め対応付けられた参照テーブルとに基づき、記憶手段に記憶された複数種の複合化プログラムから使用すべき複合化プログラムを自動特定し、当該復号化プログラムにより前記受信済み暗号化ファイルを自動復号化する機能と、を具備する。

【００１７】

『ファイル』には、文書ファイル、画像ファイル、プログラムファイル等、ネットワーク上を運ばれる種々のデータが含まれる。

【００１８】

『送信先データ』としては、例えば、ＩＰアドレス、電子メールアドレス等が挙げられる。

【００１９】

『暗号化プログラム』或いは『復号化プログラム』とあるが、これは、例えば、暗号化ソフト、復号化ソフト等として別途保存されるようにしてもよいし、この秘密通信用ソフトウェアに予め組み込まれておくようにしてもよい。

【００２０】

尚、ここでは、例えば、‘暗号化ソフト’が同一で‘暗号化鍵’が異なるような場合には「異なる暗号化プログラム」であるものとする。

【００２１】

本発明の第３実施形態によれば、各送信元又は送信先毎に異なった方式に従って、指定されたファイルを自動暗号化乃至自動復号化することができる。したがって、暗号化方式が固定となりがちであった従来のものに比して、より一層安全性の高い秘密通信が実現可能となる。

【００２２】

尚、第３実施形態においては、『暗号化プログラム』または『復号化プログラム』は、各人に対して複数のものを予め対応づけておくようにすることもできる。この場合には、その都度、複数のプログラムの中から使用すべきプログラムを特定するようにする。特定方法としては、例えば、‘暗号化された時間帯’、‘、‘その者に対する総送信回数’等に基づくものや、送信者側でその都度指定される識別コード等に基づくもの等、種々のものが挙げられるが、少なくとも、暗号化プログラムと復号化プログラムとが一体に特定される必要があることは言うまでもないであろう。

【００２３】

第３実施形態において、好ましくは、参照テーブルとして情報処理装置に別途記憶されている電子メールソフトのアドレス帳機能を利用するための電子メールソフト互換機能が具備される。

【００２４】

また、好ましくは、自動暗号化された送信予定ファイルを当該電子メールソフトによる電子メールに添付してそのとき指定された送信先へと自動送信するための電子メールソフト互換機能が具備される。

【００２５】

このような態様によれば、参照テーブルや暗号化されたファイルの送受信については既存の電子メールソフトの機能を利用することができるから、使い勝手が向上する。

【００２６】

尚、『送信予定ファイルを～電子メールに添付して』とあるが、暗号化すべきファイルが電子メール本文であるような場合も、ここで言う‘添付’に含まれるものとする。

【００２７】

第３実施形態において好ましくは、参照テーブルにおいては、１つの送信先データに対して複数種の暗号化プログラムが適用順データとともに対応づけ可能とされており、当該対応付けがなされている送信先データで特定される送信予定ファイルは、それら複数種の暗号化プログラムを適用順データに基づき順番に使用することにより多重暗号化され、また、参照テーブルにおいては、１つの送信元データに対して複数種の復号化プログラムが対応付け可能とされており、当該対応付けがなされている送信元データで特定される復号化ファイルは、それら複数種の復号化プログラムを適用順データに基づき順番に使用することにより復号化が行われるようにする。

【００２８】

このような態様によれば、より一層、通信傍受等に対する安全性が高まる。尚、より好ましくは、参照テーブルには、各送信先データまたは送信元データ毎に、電子メール本文と電子メール添付ファイルとのそれぞれについて別個に複数の暗号化プログラムまたは復号化プログラムを対応付けるようにする。

【００２９】

このような態様によれば、もっぱら、データ量が多くなりがちな添付ファイルについては多重度を少なくする、等の設定を適宜施すことにより、暗号化乃至複合化に係る処理時間を短縮することができる。

【００３０】

この場合、更に好ましくは、適用順データは、予め定められた規則に基づき適

宜自動変更されるようにする。

【００３１】

『規則に基づき適宜自動変更』とあるが、これとしては、例えば、‘日付’に基づく変更や、‘使用頻度’に基づく変更、送信者側でその都度指定される識別コード等に基づく変更等、種々のものが挙げられるが、少なくとも、暗号化するときの適用順と複合化するときの適用順とが一体となって特定される必要があることは言うまでもないであろう。

【００３２】

尚、上述の実施形態においては、例えば、以下の機能をさらに付加するようにするとより一層便利である。

（ａ）何れのデータ（ファイル）を送信し、その中のどのデータを暗号化するかをユーザが指定可能。

（ｂ）複数のファイルを送信するとき、各ファイル毎に暗号化有無、暗号化方式をユーザが適宜指定できる機能。

【００３３】

次に、本発明の第４実施形態は、ナンバーディスプレイ等の発信者通知機能を有する電話機であって、暗号化プログラムおよび復号化プログラムとを入力する手段と、発信先データと任意の暗号化プログラムとを対応づけて暗号化参照データとして予め記憶させるための手段と、発信元データと任意の複合化プログラムとを対応づけて復号化参照データとして予め記憶させるための記憶手段と、そのときの通話に係る発信先データと前記暗号化参照データとに基づきその通話に際して使用する暗号化プログラムを特定し、当該暗号化プログラムを使用して送信すべき音声信号を適宜暗号化して送信する手段と、そのときの通話に係る発信者データと前記復号化参照データとに基づきそのとき使用する複合化プログラムを特定し、当該復号化プログラムを使用して順次受信される音声信号を適宜複合化して音声出力する手段と、を有する。

【００３４】

第４実施形態において、好ましくは、参照テーブルにおいては、１つの発信先データに対して複数種の暗号化プログラムが対応づけ可能とされており、当該対

応付けがなされている発信先への送信される音声信号は、それら複数種の暗号化プラグラムに基づき多重暗号化され、また、参照テーブルにおいては、１つの発信元データに対して複数種の復号化プログラムが対応付け可能とされており、当該対応付けがなされている発信元から送信されてくる音声信号は、それら複数種の復号化プログラムに基づき多重復号化されるようにする。

【００３５】

【発明の実施の形態】

以下に本発明に係る秘密通信方法について添付図面を参照しつつ詳細に説明する。

【００３６】

まず、本実施形態で採用される秘密通信方法としての「順序対方式暗号通信」についての概略を説明する。尚、この例では、順序対方式暗号通信は、インターネットによる電子メールの通信や、通話に係る電話回線通信に採用される。

【００３７】

順序対方式暗号通信においては、送信者と受信者の順序対に対して、暗号化方式と復号化方式が一意的に決定される。そして、この方式に従った暗号通信が行われるように、通信ソフト（電子メールソフト等）の機能が拡張される。暗号化又は復号化は、暗号方式の指定欄を持つアドレス帳を利用して特定される暗号化鍵、暗号化ソフト、又は復号化鍵、復号化ソフトに基づき自動的に行われる。また、暗号解読技術の発展に合わせて、新しい暗号方式に簡単に変更可能とされる。暗号化方式は、原則として、情報の受信者が予め決定するように取り決める。

【００３８】

暗号化部分（暗号化鍵、暗号化ソフト）と復号化部分（復号化ソフト）のうち、暗号化部分の自由な再配布を認めるようにする。また、復号化部分の再配布を禁止できるようにしておく。これによって、暗号用ソフトを商業ベースで開発販売することを経済的に保証でき、優れた暗号ソフトが安定して供給されるようになる。

【００３９】

この方式は電話による通信の場合でも利用できるが、現在の電話機に記憶装置

と演算装置を付け加える必要がある。さらに、いくつかの項目について規格を統一する必要がある。

【００４０】

先ず、現在のハードウェア（パソコン等）を使用してすぐに実現できるインターネットの電子メールに関する事柄を中心に説明する。

【００４１】

２つのものＸとＹに順序を付けて並べる方法は（Ｘ，Ｙ）と（Ｙ，Ｘ）の２種類であり、これ以外にはない。この自然法則を利用する。

【００４２】

［アドレスの一意性とその順序対］

インターネット社会ではメールアドレスやＩＰアドレスなど、個人を特定するための識別記号が存在する。情報の発信者と受信者の２者を特定すれば、２つのメールアドレスから（発信者、受信者）の順序対を決定できる。

この順序対に対応して暗号化方式を決定する。（Ｘ，Ｙ）をＸさんからＹさんへの通信とするとき、このときの暗号化方式は、原則として受信者であるＹさんが自由に決定できるようにする。

さらに、ＸさんからＹさんへ送られる情報が、Ｙさんが事前に決めておいた方式で自動的に暗号化されるようにする。

Ｙさんが信頼する暗号化技術が、Ｘさんから見て信頼できる技術であるとは限らない。そこで、ＸさんがＹさんから情報を送ってもらうときは、順序対（Ｙ，Ｘ）によって決まる暗号化方式、すなわちＸさんがＹさんに対してあらかじめしてしておいた暗号化方式で暗号化して送信してもらうようにすればよい。

【００４３】

［アドレス帳の拡張］

現在、インターネットでの通信に利用するソフトにはアドレス帳があり、そこには名前、メールアドレス、組織、電話番号などが記述されている。

これを拡張して、暗号化鍵、暗号化ソフト、復号化鍵、復号化ソフトの４項目（欄）を追加する。例えば、図１（ａ）に示されるように変更する。

【００４４】

尚、同図（ａ）における記号、ＫＣax，Ｃax，ＫＰxa，Ｐxaは、それぞれ以下のように規定される。

ＫＣax…秋山氏からＸ社への通信を暗号化するときの暗号化鍵

Ｃax…秋山氏からＸ社への通信を暗号化するときの暗号化ソフト

ＫＰxa…Ｘ社から秋山氏への暗号化された通信を復号化するときの復号化鍵

Ｐxa…Ｘ社から秋山氏への暗号化された通信を復号化するときの復号化ソフト

【００４５】

ＸさんがＹさんに情報を送るとする。このとき、順序対（Ｘ，Ｙ）が決まり、これに対応する暗号化方式をこの順序対に対して一意的に決定する。

【００４６】

［秘密通信用ソフトウェアの送信時の機能］

送信する情報が与えられたら（特定されたら）、電子メールのあて先を調べて、アドレス一覧の暗号化鍵、暗号化ソフトの項目をチェックする。それが指定されていたら、暗号化鍵と送信内容を引き数として、指定された暗号化ソフトを呼び出し送信する情報を暗号化する。

あて先のアドレスと送信元のアドレスのみを記述した空のメールを作り、暗号化したものを添付ファイルとして送信する。

もちろん、アドレス帳に記載されていない相手や、アドレス帳に記載されていても暗号化項目が指定されていない場合は、暗号化しないでそのままメールを送ることにする。この状態では、暗号文を送っても相手が解読できないためである。尚、送信時の機能は、図２のようになる。

【００４７】

［秘密通信用ソフトウェアの受信時の機能］

暗号化されたメールの受信時には、発信者のメールアドレスとアドレス帳に基づき発信者を特定し、その発信者の項目に復号化鍵と復号化ソフトが与えられていたら、復号化鍵と添付ファイルを引数として復号化ソフトを呼び出し、復号化を行う。そして、復号化された情報を表示する。もちろん、アドレス帳に記載されていない相手や、アドレス帳に記載されていても復号化項目が指定されていなければ復号化しないでそのままメールを開くようにする。尚、受信時の機能は、

図３のようになる。

【００４８】

上述のような機能をもった秘密通信用ソフトウェア（ハードウェアでもよい）を作成する。尚、より具体的な一例として、そのように構成されたソフトウェアをパーソナルコンピュータに適用することにより実現される電子メール通信に係るコンピュータ（ＣＰＵ）の動作内容を、図４、図５、図６のフローチャートにそれぞれ示す。

【００４９】

図４は、電子メール送信時におけるＣＰＵの動作内容を示すフローチャートである。この例では、市販のメールソフトを介して通常の電子メール（送信先アドレス、本文、添付ファイル等を含む）が作成されたのち（ステップ４０１）、所定の暗号化指示がなされると（ステップ４０２ＹＥＳ）、作成された電子メールの内容が自動的に暗号化されて送信される（ステップ４０３）。尚、暗号化指示がなされず、通常の送信指示があった場合には（ステップ４０２ＮＯ）、通常のメール送信処理が行われる（ステップ４０４）。

【００５０】

図５は、ステップ４０３に示す自動暗号化処理の詳細を示すフローチャートである。自動暗号化処理においては、まず、ステップ４０１において作成された電子メールの送信先アドレスを読み込む（ステップ５０１）。次いで、読み込まれたアドレスに基づき先に図１で示したような予め機能拡張されたアドレス帳を検索して、その送信先に対応づけられた暗号化方式（暗号化鍵、暗号化ソフト）を特定する（ステップ５０２）。尚、暗号化方式が対応づけられていないような場合には（ステップ５０３ＮＯ）、例えば、‘暗号化方式が指定されていません’等のエラーメッセージがディスプレイ等を介して表示されるようにする（ステップ５０５）。

【００５１】

ステップ５０３において暗号化方式が特定されると（ステップ５０３ＹＥＳ）、特定された暗号化鍵・暗号化ソフトが読み込まれ、それらに基づき、電子メールの本文および添付ファイルとがそれぞれ別個に暗号化される（ステップ５０６

）。

【００５２】

尚、暗号化キー，暗号化ソフト、及び後述する復号化キー、複合化ソフトは、予めコンピュータのハードディスクに記憶されたものである。

【００５３】

ここで、ステップ５０６で示される暗号化処理が何らかの理由（例えば暗号化不可能なデータ等の混在等）により正常に行われなかった場合には（ステップ５０７ＮＯ）、例えば、‘「……（データ）」は暗号化できません’等のエラーメッセージがディスプレイ等を介して表示されるようにする（ステップ５０９）。

【００５４】

一方、暗号化処理が正常に終了すると（ステップ５０７ＹＥＳ）、当該電子メールには、それが暗号化されたデータを含む電子メールであることを受信者側で自動特定するためのデータ（暗号化識別コード）が、例えば暗号化された本文データの先頭等に付される（ステップ５０８）。

【００５５】

次いで、ディスプレイ等を介して、暗号化済みの電子メールを送信するか否かを確認するメッセージ‘暗号化が完了しました。送信を行いますか？’（併せて‘送信する’，‘送信しない’）が表示される（ステップ５１０）。

【００５６】

ここで、カーソル等を介してユーザにより‘送信しない’が選択されると（ステップ５１１ＮＯ）、暗号化された電子メールは直ちには送信されず、一旦、所定メモリに保存される（ステップ５１３）。

【００５７】

一方、‘送信する’が選択されると（ステップ５１１ＹＥＳ）、暗号化された電子メールが電子メールの送信手順（プロトコル）に従って通常通り送信されることとなる（ステップ５１２）。尚、この電子メール送信処理には、この例では電子メールソフトの送信機能が使用される。

【００５８】

図６は、電子メールの開封処理に係るＣＰＵの動作内容の詳細を示すフローチャートである。

【００５９】

受信された電子メールを開く際には、本実施の形態では、まず、その電子メールが暗号化されたものであるかを自動判別する。すなわち、この例では、開封が要求された電子メールについて、先に図５のステップ５０８において添付された暗号化識別コードの有無が確認される（ステップ６０１）。

【００６０】

ここで、暗号化識別コードが無いと判断されたときには（ステップ６０１ＮＯ）、通常の開封処理がなされる（ステップ６０３）。

【００６１】

一方、ステップ６０１において、暗号化識別コードが認められると（ステップ６０１ＹＥＳ）、複合化処理が開始される。

【００６２】

複合化処理においては、先ず、その電子メールの送信者（発信元）のアドレスが読み込まれる（ステップ６０２）。次いで、読み込まれたアドレスに基づき先に図１で示したようなアドレス帳を検索して（ステップ６０４）、その送信者に対応づけられた復号化方式（復号化鍵、復号化ソフト）を特定する。ここで、復号化方式が対応づけられていないような場合には（ステップ６０５ＮＯ）、例えば、‘複合化方式が指定されていません’等のエラーメッセージがディスプレイ等を介して表示されるようにする（ステップ６０７）。

【００６３】

復号化方式が特定されると（ステップ６０５ＹＥＳ）、特定された復号化鍵・復号化ソフトが読み込まれ（ステップ６０６）、それに基づき、電子メールの暗号化された本文および添付ファイルとがそれぞれ別個に複合化される（ステップ６０８）。

【００６４】

ここで、ステップ６０８で示される複合化処理が何らかの理由（例えば複合化不可能なデータ等の混在等）により正常に行われなかった場合には（ステップ６

０９ＮＯ）、例えば、‘複合化エラーが発生しました’等のエラーメッセージがディスプレイ等を介して表示されるようにする（ステップ６１１）。

【００６５】

この例では、暗号化処理が正常に終了したときには（ステップ６０９ＹＥＳ）、暗号化された電子メールは複合化された後の電子メールに置きかえられる（更新）。尚、暗号化された電子メールは、複合化されたものとは別に引き続き保存されるようにしてもよい。

【００６６】

尚、上述のフローチャートによる説明では、市販の電子メールソフトを拡張して使用するものとしたが、上述した秘密通信用ソフトウェアに専用の電子メールソフトを予め一体化しておくようにしてもよい。

【００６７】

また、復号化処理のタイミングは、電子メールの開封要求があったときとしたが、電子メールの受信時あるいは受信後直ちに自動的に行われるようにしてもよい。

【００６８】

また、上述のフローチャートによる説明では、電子メール作成後、本文や添付ファイルを自動暗号化するものとして説明したが、これは、電子メールのそのような構成（もっぱらアドレス、本文、添付ファイルに分類される）に対応して、作成後の電子メールを自動暗号化することを前提とした構成であり、これとは別に機能として、電子メール以外のファイルをその都度指定される送信先識別コード等に基づき自動暗号化するようにもできる。このような場合には、暗号化されたファイルは電子メールの添付ファイルとして添付されて送信されるようにすればよい。

【００６９】

［使用できる暗号の種類と特徴］

暗号には、大きく分けて秘密鍵方式と公開鍵方式の２種類があるが、どちらも利用可能である。尚、参考までに、社会的な評価が高く、専門家が有効と認めるような暗号化ソフトの種類は１００種類程度と考えられる。暗号化鍵と暗号化ソ

フトが統一された形で実現されたものは、実用上の問題が生じると考えられる。それは、暗号化鍵のサイズを１Ｋバイト程度とすれば、統一されたものは１Ｍバイトから１０Ｍバイト程度になるためである。すなわち、このサイズのものを、例えば１００００人分保存するには１００Ｇバイトのメモリが必要になり、１０Ｇバイト程度のハードディスクでは保存しきれない。しかし、共通の暗号化ソフトを利用できれば、暗号化鍵が１００００人分あってもそのサイズは１０Ｍバイト程度で済む。理論上は、暗号化鍵と暗号化ソフトを分離しなくてもよいが、現在のハードウェアの状況に適しているとの理由で、暗号化鍵と暗号化ソフトを分離する方式について記述する。

【００７０】

本実施の形態では、暗号用の商用ソフトは、次のような構造を持つものとして制作される。

（１）暗号化鍵の作成機能をもち、鍵の自由な配付が認められている。

（２）暗号化ソフトの再配布が認められている。

（３）復号化鍵の作成機能をもつ。

（４）復号化ソフトの再配布を禁止できる。

【００７１】

この（１）から（４）を満たすようにすることで、秘密鍵方式でも公開鍵方式でも、どちらも利用することができる。そして、図７に示すように、暗号化部分だけを配付し、復号化部分は配付しないようにする。これは、復号化部分を配付すると、だれかがネットワークの途中でその復号化部分をこっそりコピーしてしまうことが可能となるためである。そうなると自分あての暗号通信が、この復号化部分を不正に入手した人によって通信の途中で解読されてしまう。これでは暗号も役に立たない。

【００７２】

復号化ソフトの再配布を禁止できれば、暗号化ソフトの利用者がそれぞれソフトを購入することになるため、商業的にソフトを制作販売することが可能となり、結果、より優れた暗号ソフトの開発も可能となる。

【００７３】

暗号化ソフトは自作してもよいが、安全な暗号化ソフトを作成するにはかなりの時間と努力を必要とする。暗号ソフトは既にかなりの種類が存在し、日本が世界をリードしているところもある。社会的に評価の高いものを選ぶのが現実的な選択と思われる。

【００７４】

［秘密鍵方式を使う場合］

秘密鍵方式を使うときは、秘密鍵と暗号化ソフトを事前に配付しておくことになる。具体例として、シーザー暗号方式の場合を示す。

【００７５】

例えば、秋山氏はシーザー暗号を使うことにし、伊藤氏からの情報は暗号化鍵（－１）で、斉藤氏からの情報は暗号鍵（２）で暗号化してもらうことにしたとする。尚、図８（ａ）～（ｃ）は、このような場合における秋山氏、伊藤氏、斉藤氏のそれぞれのアドレス帳の内容の一例をそれぞれ示すものである。

【００７６】

秋山氏は、暗号化鍵（伊藤氏：‘－１’，斉藤氏：‘２’）と暗号化ソフト（Ｃ）を伊藤氏と斉藤氏に送る。伊藤氏、斉藤氏は自分のアドレス帳の暗号化欄にそれらを登録する。

【００７７】

これにより、例えば、伊藤氏から秋山氏への送信データ「ＩＢＭ（データ内容）」は、鍵（－１）で暗号化され、「ＨＡＬ」となる。伊藤氏からの暗号文「ＨＡＬ」は、秋山氏の伊藤氏の通信に対する鍵（１）で復号化され「ＩＢＭ」に戻る。斉藤氏から秋山氏への通信「ＩＢＭ」は、鍵（２）で暗号化され、「ＫＤＯ」となる。暗号文「ＫＤＯ」は鍵（－２）で復号化され、「ＩＢＭ」に戻る。つまり、この例では暗号化鍵の示す値（数）だけアルファベット文字を先に進め、復号化鍵の示す数だけ元に戻す形になっている。

【００７８】

図９は、このような秘密鍵方式利用による通信態様を模式的に示したものであるが、この秘密鍵方式では、暗号化のための鍵を安全な方法で相手に伝達することが特に重要となる。そのため、電話で連絡を取ったり、実際に会ったりして鍵

を交換する方が好ましい

【００７９】

［公開鍵暗号方式を使う場合］

公開鍵方式を使うときは、暗号化した情報を送ってもらいたい相手全員に公開鍵を送っておけばよい。また、暗号化ソフトも同じものを配付しておく。もちろん、公開鍵方式にもその実現形態はいろいろあるので、相手ごとに別の公開鍵方式による暗号化ソフトを利用することも可能である。

【００８０】

具体例として、離散対数を利用した場合を示す。素数ｐ，ｑを選び、ｎ＝ｐｑとする。Ｋ＝１ｃｍ（ｐ－１，ｑ－１）として、ｇｃｄ（ｄ，Ｋ）＝１となるｄを選ぶ。次に、ｅｄ＝１（ｍｏｄ　Ｋ），０＜ｅ＜Ｋとなる整数ｅを計算する。秋山氏は、ｅ，ｎを公開し、暗号化ソフト（Ｃ）を送付する。ｄは秘密とし、自分のアドレス帳にｎとともに登録しておく。尚、図１１は、このような公開鍵方式利用における通信態様を模式的に示したものである。

【００８１】

尚、この場合の秋山氏のアドレス帳の一例を示せば、図１０（ａ）に示すようになる。また、秋山氏が、暗号化鍵と暗号化ソフトを伊藤氏と斉藤氏に送ったとすれば、伊藤氏、斉藤氏のアドレス帳は図１０（ｂ）、図１０（ｃ）に示すようになる。

【００８２】

数ｘを送信するとすれば、伊藤氏と斉藤氏の持っている暗号化ソフトＣはｅ，ｎを使って、ｘｅ≡ｃ（ｍｏｄ　ｎ）を計算し、このｃを秋山氏へ送信する。受け取った秋山氏は、ｘｄ≡ｘ（ｍｏｄ　ｎ）によってｘを得る。すなわち法ｎでｃのｄ乗を計算して、ｘを得る。

【００８３】

図１１に示されるような公開鍵にも問題はある。それは、その公開鍵を所有しているのが、本当は誰なのかということを確認することが困難なことである。

【００８４】

公開鍵に証明書をつけて、その公開鍵の所有者が誰なのかを明らかにする方法

もあるが、この証明書を発行する認証局が興信所やデータベースで調べたりして独自の調査を行って証明書を発行する場合は、発行費が高額になる。

【００８５】

普通の証明書で示される内容は、本人がそのように主張しているということを示しているにすぎない。一番確実なのは、誰かと直接会って本人から公開鍵を受け取ることと思われる。

【００８６】

ネットワーク上で知り合っただけで、ネットワークアドレスと名前だけしか知らないような場合でも、本人の身分や本当の名前などを気にしないで、相手が「この方式で暗号化して情報を送ってくれ」と言っているなら、それで暗号化して送ってやればよいと考えることもできる。

【００８７】

［暗号化鍵と暗号化ソフトの配付方法］

情報を送ってもらう相手に、あらかじめ暗号化鍵と暗号化ソフトを所持してもらう必要がある。直接会ってフロッピーディスクなどに記録したものを渡すとか、それらを郵送するなどの方法や、秘密鍵を公開鍵暗号方式などによって暗号化して、それをネットワークで送るなどの方法がある。なお、暗号化鍵を交換するときの問題点については、例えば、翔泳者発行の『暗号化によるセキュリティー対策ガイド』等を参照されたい。

【００８８】

やはり、直接会ってお互いに自分の選んだ暗号化ソフトと暗号化鍵を交換するのが簡単で確実と考えられる。

【００８９】

［暗号化鍵と暗号化ソフトの登録］

暗号化鍵と暗号化ソフトを受け取った人は、自分のアドレス帳に登録する。例えば、秋山氏が伊藤氏との通信で暗号を利用することにした仮定する。順序対（伊藤、秋山）に対応する暗号化方式が決まる。秋山氏が伊藤氏からの通信を受信するときの暗号化方式をＣ（ｉ，ａ）とする。秋山氏は、伊藤氏に会って、暗号化ソフト（Ｃia）と暗号化鍵（ＫＣia）を手渡す。伊藤氏は、アドレス帳の秋山

氏の項目に、この暗号化ソフトと暗号化鍵を登録し、暗号化ソフトと暗号化鍵をハードディスク内に記録しておく。この場合の伊藤氏のアドレス帳は、例えば図１２（ａ）のようになる。

【００９０】

［復号化ソフトの登録］

秋山氏は、伊藤氏からの情報を受信するときに利用する暗号方式を決定したので、これによって決まる復号化鍵（ＫＰia）と復号化ソフト（Ｐia）を、アドレス帳の伊藤氏の欄にある復号化鍵、復号化ソフトの項目に登録する。この場合の秋山氏のアドレス帳は、例えば、図１２（ｂ）のようになる。

【００９１】

このアドレス帳により、秋山氏は伊藤氏からの通信を（Ｃia）によって暗号化した形で送ってもらうことができる。また、届いた情報は、（Ｐia）によって自動的に解読（復号化）される。

【００９２】

尚、秋山氏は、同じ暗号化方式、同じ暗号化鍵を伊藤氏以外の人との通信で利用することができ、また、暗号化ソフトは同じでも、暗号化鍵を変えてほかの人と通信を行うこともできる。

【００９３】

また、全く別の方式で暗号化した通信を行うこともできる。なぜなら、暗号化方式とその実現形態は送信者と受信者の順序対で決まるためである。同様に、伊藤氏が、秋山氏から送られてくる情報の暗号化に別の方式を選択できることも明らかである。

【００９４】

［復号化ソフト再配布禁止の意義］

暗号化ソフトが、同時に復号化ソフトとして機能することがないようにしておけば、暗号化ソフトを購入して本実施形態の秘密通信方法を利用する人は、それぞれ復号化ソフトを必要とするので、個別に暗号化ソフトを購入しなくてはならないことになる。なぜなら、復号化ソフトは再配布が禁止となっているためである。このことは、暗号化ソフトの商業的開発を保証し、より安全な通信のための

経済的基盤となり得る。暗号化ソフトの開発には長時間の研究が必要であり、経済的保証がなければ優れた暗号化ソフトを開発することはできない。

【００９５】

［暗号化ソフトの名前の一意性］

異なる暗号化ソフトに同じ名前が付くと、ハードディスクの中に保存するときに問題が生じる。したがって、暗号化ソフトの開発者が持つ一意的な識別記号（メールアドレスなど）をその暗号化ソフトの名前に使用して、名前の衝突が起きないようにする必要がある。

【００９６】

［商業的利用］

証券会社（Ｘ社）は、顧客に対し有料で情報提供を行うとする。ある顧客が自動車会社に関心を持っていたとする。その顧客にとっては、自動車会社の新車開発情報などを自分だけに知らせてもらえるなら、高い値段が付いていても購入する価値のある情報と考えられる。

【００９７】

しかし現実には、この自分だけが知りたい情報の伝達がネットワーク上で盗難や改竄を受けるおそれがあるので、今ひとつ不安がある。そこで、Ｘ社はこの順序対方式暗号通信を採用したとする。Ｘ社の顧客アドレス一覧は、例えば、図１（ｃ）に示されるようになる。

【００９８】

Ｘ社は、顧客の関心を持つ経済分野の情報を有料で配信するとする。顧客が暗号化方式を決定するのが原則であるが、社会的に評価の高い暗号ソフトを１０種類程度は紹介する必要もある。逆に、顧客からの注文などを受け取るための暗号方式を決定する。これは顧客の購買力によって方式を変えることもできる。

【００９９】

できれば、異なった暗号化鍵を顧客の数だけ作り出せるものが便利である。しかも、復号化鍵はお客ごとに異なるとしても、復号化ソフトは同じものが利用できるような暗号ソフトがよいであろう。ここにも、復号化鍵と復号化ソフトを分離できる形のメリットが見いだせる。

【０１００】

価値ある経済情報は自分だけに知らせてほしいと思うし、この情報がネットワーク上で盗聴されたり改竄されたりすることは防ぎたい。この方式は、顧客自身の責任で自分のための情報を保護できる。これによって、情報にさらなる付加価値を付けることができる。これは、経済的に価値の高い情報を伝えるためには不可欠の方式となる。

【０１０１】

［個人による利用］

この方式を個人が利用する場合のアドレス帳は、図１（ａ），図１（ｂ）に示されるような形になる。個人で利用する場合は、経済的負担を考える必要がある。

【０１０２】

公開鍵暗号などの場合は、同じ暗号化鍵を配付すれば済むので、復号化鍵、復号化ソフトは１種類で済ませることもできる。また、商業的な通信と友人間の通信に分けて、別の公開鍵方式を採用することもできる。

【０１０３】

秘密鍵方式では、相手ごとに異なる秘密鍵を作成し、これに対応した復号化鍵を自分のアドレス帳の復号化鍵の欄に記録しておくようにする。鍵が異なっても同じ暗号化ソフト、同じ復号化ソフトを使用することができるので、ハードディスクなどの資源を節約することもできる。無論、通信相手ごとに暗号化方式を変えても良い。

【０１０４】

暗号化ソフトが、暗号化鍵と一体化されていると比較的大きなサイズとなり、これをアドレス帳に記載された人数分だけ自分のハードディスクの中に用意することになる。人数が増えると、２０Ｇバイト程度のハードディスクでは容量が不足する。そこで、サイズの小さな暗号化鍵は、アドレス帳に記載された人数分だけ用意するにしても、サイズの大きな暗号化ソフトは、共通に利用できることが望ましい。

【０１０５】

現状で有効と認められる暗号ソフトは、１００程度と思われる。暗号化ソフトを共通で利用できるなら、ハードディスクに暗号ソフトを１００種類だけ置いておけば済む。また、暗号化ソフトだけを、雑誌の付録などで配付することも可能であるので、実際にはそれを入手し、暗号化鍵だけをやりとりすることも、現実的な方法と思われる。

【０１０６】

電子メールを送るときには、あて先のアドレスと発信者のアドレスが最初に決まり、発信者と受信者の順序対が決まることになる。この順序対に対応した暗号化方式によって自動的に暗号化される。

【０１０７】

受信者の方では、発信者のアドレスとあて先である自分のアドレスの順序対から復号化方式を決定できるので、暗号化されて送付された情報を自動的に復号化できる。

【０１０８】

例えば、秋山氏は伊藤氏からの情報を受信するときに利用する暗号化方式を決定する。秋山氏は伊藤氏との通信で使う暗号化鍵（ＫＣia）、暗号化ソフト（Ｃia）、復号化鍵（ＫＰia）、復号化ソフト（Ｐia）を用意し、このうち暗号化鍵（ＫＣia）、暗号化ソフト（Ｃia）に関する情報を事前に伊藤氏に送っておく。伊藤氏はアドレス帳の秋山氏の項目に、暗号化鍵と暗号化ソフトを登録しておく。

【０１０９】

伊藤氏から秋山氏へのメールは、秋山氏が決めた暗号化方式（Ｃia）と暗号化鍵（ＫＣia）によって暗号化される。これを受け取った秋山氏の通信用ソフトは、送信者のアドレスと、自分のアドレスを判別できるので、これによって復号化方式（Ｐia）と復号化鍵（ＫＰia）を自動的に選び、この方式で復号化する。

【０１１０】

逆に、伊藤氏は秋山氏からの情報を受け取るための暗号化方式を決定する。もちろん、この方式は伊藤氏が自由に決定できる。秋山氏からの情報を受け取るために使う暗号化鍵（ＫＣai）、暗号化ソフト（Ｃai）、復号化鍵（ＫＰai）、復

号化ソフト（Ｐai）を用意する。このうち、暗号化鍵（ＫＣai）、暗号化ソフト（Ｃai）を事前に秋山氏に伝えておく。

【０１１１】

秋山氏から伊藤氏へのメールは、伊藤氏が決めた暗号化方式（Ｃai）と暗号化鍵（ＫＣai）によって暗号化される。受け取った伊藤氏は、秋山氏用の復号化鍵（ＫＰai）と復号化ソフト（Ｐai）を使って解読する。

【０１１２】

［暗号方式の更新］

暗号技術の進歩は驚くほど早く、暗号解読技術も同時に進歩している。１つの暗号化方式が安全であるのはせいぜい５年間ぐらいと考えられる。したがって、情報の受信者自身が利用する暗号技術を自由に更新できるのが好ましい。

【０１１３】

この実施の形態で示される順序対方式暗号通信によれば、変更が情報の受信者の意志で自由にできる。そのため、その時点での最も優れた暗号技術を選択することも可能である。

【０１１４】

新しい暗号方式を利用すると決めた者は、新しい暗号ソフトを購入し、その暗号化部分を自分のアドレス帳に記載されている人に配付し、登録更新を依頼する。また、自分のアドレス帳の復号化部分の登録内容を更新する。

【０１１５】

もちろん、簡単な暗号化でよい人や、暗号化が必要ない人もいるであろうが、自分の部屋の鍵を自分で決めるように、自分の意志で、自分の扱う情報の価値にあった暗号化方式を決定することが重要と思われる。

【０１１６】

［機能の拡張］

暗号化、復号化の鍵を複数にして複数回の暗号化を重ねることも可能である。特に有料での情報配信では、顧客の決定する暗号方式以外に、会社から見て最低限の強度を持っていると認められる暗号化方式も採用して、情報を少なくとも２重に暗号化（多重暗号化）するのが好ましい。以下に多重暗号化について詳述す

る。

【０１１７】

簡単に多重暗号化ができるようにするには、それを自動化する必要がある。そこで、図１３に示すようなアドレス帳を考える。同図に示されるように、各人（送信先）毎に複数の暗号化欄（暗号化１、２、…）と復号化欄（復号化１、２、…）を設け、この欄で指定されたソフトとキーを使って通信内容を複数回暗号化する。

【０１１８】

より詳細には、通信相手ごとに、それぞれ複数の暗号化ソフトと暗号化キー、復号化ソフトと復号化キーとを登録しておく。この表に従って、送信時や受信時に自動的に暗号化、復号化が行われる。図１４は、このような多重暗号化、（多重）複合化の処理手順を示したものであり、同図に示す例では、送信時には５回（５段）の暗号化処理がなされており、受信時には、送信時と逆の手順で同様に５回に渡り復号化処理がなされている。尚、多重暗号化の際、各回で使用される暗号化ソフトは必ずしも全て異なったものとする必要はない。例えば、暗号化ソフトとして１つのソフトのみを用いて、各回で暗号化キーのみを異ならせるようにしてもよい。

【０１１９】

［多重暗号化による効果］

現在、公開鍵方式での暗号化が主流となっているが、将来にわたって安全であるという保証はない。暗号化の技術よりも解読技術の方が急速に進歩することもあり得る。古い暗号化方式を含めて考えれば、利用できる暗号化の方式はかなり多い。これらを組み合わせることにより、処理時間の増加よりも、解読に必要な時間は急激に増加する。これは、暗号化技術の進歩の遅れを補ってくれる。

【０１２０】

上記した例の場合、例えば１００種類の暗号化方式の中から、５つ選んで使用する。どの５つをどの順序で使用しているかが不明ならば、解読に要する時間は、１００の５乗倍になる。処理時間は５倍になるだけなので、ＣＰＵの処理速度が日々向上していることを考えればこの処理時間５倍は５万円の新しいコンピュ

ータを買えば解決してしまう問題となる。

【０１２１】

しかも、アドレス帳に記載された内容に従って自動的に暗号化や復号化が行われるので、利用者が面倒な操作をする必要がない。

【０１２２】

［処理速度の向上］

アドレス帳に、多重暗号化に係る多重度調整項目を追加し、一つのメールの本文とその添付ファイルでは、暗号化の多重度を変えることもできる。これによって、画像ファイルなどの暗号化の多重度を減らして、全体の処理速度を軽減することもできる。

【０１２３】

例えば、図１５に示されるアドレス帳によれば、宇山宛のメールの本文は登録されている暗号化ソフト（例えば暗号化１～暗号化５の欄までが存在すると仮定する）のうち、１，２，３，４，５番の欄に示されるものを使って、多重暗号化されるが、添付ファイルは４，２番目のものを使って暗号化される。また、宇山からのメールの本文は、復号化のうち１，３番のものを使って復号化され添付ファイルは５番のものを使って復号化される。

【０１２４】

このように、部分ごとに必要な多重度を設定することで、暗号化、復号化にかかる時間を節約できる。

【０１２５】

［長期固定化の排除］

長期間にわたって、同じ暗号が同じ順序で利用されていると、解読される可能性が増える。そこで、スケジュールファイルを設定し、長期にわたる固定化を避ける。例えば、図１５に示されるように、１ヶ月ごとに暗号化の順番をこのスケジュールファイル（規則）に従って自動的に変える（この例では、多重暗号化におけるソフト、キーの‘使用順’を変更（置換）する）ようにする。例えば、最初は、１２３４５の順番だったものは、次の月は、３１５２４の順番となり、次は、５３４１２（図示省略）の順番となる。

【０１２６】

さらに一定期間（例えば３年）が過ぎたら、使用する暗号を新しい方式のものに更新することを勧めるメッセージや、段数を増やすように勧めるメッセージが出るようにするとよいであろう。

【０１２７】

尚、暗号化方式の固定化を避けるための自動変更には、この他にも種々の態様が考えられる。他の一例としては、例えば、特定送信先への所定回数の送信がある毎に（この場合には送信回数をカウントし、カウント値が所定数になったら）、その送信先について使用するソフト及び／又はキー（暗号化欄）を自動変更（例えば予め各人毎に対応づけられた複数のソフト及び／又はキーの中から予め定められた規則に従い任意のものを新たに選択）するものが挙げられる。この場合には、その受信者側のアドレス帳の復号化欄も、同様のタイミング（受信回数をカウント）と規則にしたがって変更が行われるようにする。

【０１２８】

［電話の場合］

上述の順序対方式暗号通信は、電話にも適用できる。電話でこの方法を利用する場合は、いくつかの通信規格を決定する必要がある。第１は、音声をデジタル化するときのサンプリングレートの規格であり、第２は、デジタル化した音声を一定量ごとに暗号化するときのその量に関する規格である。

【０１２９】

この２点が決まれば、ナンバーディスプレイ等の電話番号通知機能を利用して、送信者と受信者の電話番号が特定できるから、この順序対によって決まる暗号化により、電話においても秘密通信が可能となる。

【０１３０】

家庭用の電話機の場合は、記憶装置と演算装置を組み込むことは簡単であり、電源の問題も心配なく、暗号化と復号化の処理速度の問題を解決するだけで済む。

【０１３１】

携帯電話の場合は、メモリスティックなどで記憶装置の問題を解決する。暗号

方式を簡単にすることで演算装置の大きさの問題点も解決できる。

【０１３２】

例えば、データが１０２４ビットごとに暗号化されるとする。暗号化鍵と復号化鍵をこのビット長に相当する文章とし、送信者と受信者で同一の文章を使用する。暗号化方式と復号化方式はＸＯＲとする。暗号化も復号化もデジタルデータと鍵となる文章の１０２４ビットごとのＸＯＲによって実現できる。文章は記憶装置に書き込んでおけばよい。ＸＯＲだけなら簡単な回路で実現できるので、本格的な演算装置を使う必要はない。お互いに自分の好きな文章を選んで相手に登録してもらえばよい。

【０１３３】

残る問題点として、第３は、記憶装置と演算装置を組み込んだ電話機の製作がある。これは新しい需要を喚起することになる。このようなコンピュータに近い電話機の製作販売は日本の景気回復にも役立つと思われる。

【０１３４】

尚、上述のような電話での利用に際しては、携帯電話などにおいても、暗号化には利用者の独自部分が必要となる。なぜなら、電話会社によって与えられたものだけでは、電話に関して十分な知識とお金がある者によって簡単に盗聴されてしまうからである。順序対方式暗号通信の考えを使えば、たとえ盗聴されても通信の秘密を守ることができる。

【０１３５】

現在の携帯電話機での演算装置の能力を考えるとき、リアルタイムの処理ができるようにするには、暗号化方式を制限する必要がある。伝達されるものが人間の音声であることを考えれば、上述したように、文字列とデジタル化された音声信号との排他的論理和を選ぶことが現実的な選択である。

【０１３６】

多重暗号化の方法を利用して、文字列を２重にし、片方は全角文字列、もう一方は半角文字列の場合のようにそれらの間に共通な文字がないようにする。それぞれの文字列の長さは互いに素となるようにすることによって、強力で高速な暗号化を実現できる。

【０１３７】

音声信号が長いときは、暗号化キーとなる文字列は繰り返して同じものを利用する事になる。１つの文字列では、文字列の長さが短いとこの繰り返しが多くなる。これは暗号化された音声信号が解読されてしまう可能性が増す。単純に考えれば、キーとなる文字列を長いものにして、繰り返しを防げばよいのだが、単純に長い文字列を保存するのではなく長さが互いに素である複数の文字列を利用すれば、少ないメモリーの使用でも、より長い文字列と同じような効果を得ることができる。以下に、具体例を示す。

【０１３８】

文字列を２つ利用する場合を考える。電話では、処理速度の問題が一番大きい問題である。演算の中で可逆性があり高速に行えるのが排他的論理和（ＸＯＲ）を取る操作である。０ＸＯＲ０＝０、０ＸＯＲ１＝１、１ＸＯＲ０＝１、１ＸＯＲ１＝０のように計算される。これを使って順序対方式で考えれば基本的な形態は次のようになる。

【０１３９】

Ｓさんと、Ｒさんの電話での会話を考える。例えば、Ｓさんの電話のメモリーの内容を図１７（ａ）、Ｒさんの電話の内容を図１７（ｂ）にそれぞれ示されるものとする。

【０１４０】

Ｓさんが、Ｒさんに向けて＜今日は…＞と話しかけたとする。これに対するアナログ音声信号をデジタル化した結果が、0x1216，0x0800，0x1182，…だったとする。文字コードとして、ＪＩＳコードを使えば、＜あおいそら…＞は、0x2422，0x242A，0x2424，0x243D，0x2469，…となり、＜0aufefhgoo…＞は　0x4f，0x62，…となる。

0x1216をビットごとの表現で見れば　0001 0010 0001 0110であり、

0x2422をビットごとの表現で見れば　0010 0100 0010 0010である。

0x4f 0x61をビットごとの表現で見れば　0100 1111 0110 0001である。

この３つのＸＯＲをとれば、0111 1001 0101 0101、１６進数では0x7955となる。これを続ける。このようにして得られる数値列、0x7955，…を送信する。

【０１４１】

Ｒさんは、この値0x7955，…を受け取る。まず、0x7955＝0111 1001 0101 0101について、保存してある文字コード＜あおいそら…＞は、0x2422，0x242A，0x2424，0x243D，0xw2469，…、＜0aufefhgoo…＞は、0x4f，0x62，…であり、これらを使って、ＸＯＲをとる。これを続けると、元の音声信号のデジタル化されたものが得られる。デジタル信号をアナログ信号に戻せば＜今日は…＞というＳさんの声が聞こえる。

【０１４２】

Ｒさんの返事＜Ｓさんですか…＞は、暗号化キー＜Abcdefg…＞と＜なにかな…＞によって暗号化され、Ｓさんの電話機の中で、復号化キー＜Abcdefg…＞と＜なにかな…＞によって復号化され、Ｒさんの声＜Ｓさんですか…＞が聞こえることになる。

【０１４３】

途中で、盗聴した人は、２重の文字列が判らないと音声を復元できない。同じ言葉を話すとしても、音声化したときの波形は人によって異なり、それと２重文字列とのＸＯＲをとるので、解読は困難となる。

【０１４４】

利用者自身が設定できるもので暗号化されるので、電話に関する知識が十分にある盗聴者にとっても解読は極めて困難となる。

【０１４５】

［文字列と文字列の関係］

文字列を２重の場合は、片方は全角文字列もう一方は半角文字列のように、それらの間に共通な文字がないようにする。これは、共通な文字が重なるとその部分は暗号化されなくなってしまうからである。

【０１４６】

２つの文字列は、長さが互い素（最大公約数が１）になるようにして、長さの最小公倍数が、大きくなるようにすべきである。

【０１４７】

例えば、図１８（ａ）に示すように、長さ３の文字列（はてな…）と長さ５の

文字列（あおいそら…）を使えば、長さ１５のキーを使っているのと同じになる。

【０１４８】

このときは、１５文字分ごとに使用するキーの繰り返しが起こる。この繰り返しはなるべく起こらない方がよい。

【０１４９】

もし、キーとして、９９１文字と９９７文字の２つの文字列を使用することは、９８８０２７文字分の文字列キーを１つ使って暗号化することに相当する。

【０１５０】

［３つの文字列キーの場合］

３つの文字列を使う場合の例では、１０２４，９９７，９９１をそれぞれの文字列の長さとすれば、１つの文字列で暗号化した場合と比べると、長さ１０１１７３９６４８の長さの文字列の使用した場合に相当する。このことから、複数の文字列を使う場合それらの長さが互いに素になるように選ぶべきである。

【０１５１】

３つの文字列は、例えば図１８（ｂ）に示すように、全角文字の系列（キー１）、アルファベットの系列（キー２）、数字の系列（キー３）を混合し、複雑化を図るべきである。

【０１５２】

尚、補足すれば、電話機における秘密通信に関しては、さらに、次のような機能があると便利である。

１　設定した文字列を電話局や中継基地を介さずに、ケーブルなどで直接相手の電話機に送る機能。（例えば、ａｕのＣメール）

２　暗号化キーの部分は＊＊＊＊＊＊＊のように表示されてユーザＩＤがなければ変更できないような機能。

３　入力した文字列の長さが互いに素であるか否かをチェックする機能。

４　複数の文字列における同じ文字の重なりの有無を確認する機能。

５　一定の期間（例えば６ヶ月）過ぎたとき、キーとなる文字列の更新を促すメッセージが表示される機能。

６　時刻と相手の氏名や電話番号などからキーとなる文字列を適当な長さで生成してくれる機能。

【０１５３】

以上説明した実施形態によれば、固定式となりがちだった従来の秘密通信方法に比して、より安全性（秘密性）の高い秘密通信が簡易に実現される。また、暗号解読の技術の発展に対応して、新しい暗号化方式に適宜切り替えることも容易であり、これによりその安全性をより一層高めることも可能となる。このため、通信全般における将来の普及も期待され、安全性の高いネットワーク社会の実現にも貢献することができる。

【０１５４】

尚、上述の説明では、受信者により予め指定された暗号化方式を使用して暗号化を行うものとして説明したが、必ずしもこれに拘束される必要はない。受信者側における復号化が可能であるならば、送信者側で送信したいファイル毎に暗号化方式を適宜決定するようにしてもよい。

【０１５５】

また、上記実施形態における暗号化方式は、例えば、各送信先毎に複数の暗号化方式をランク分けして用意（対応付け）しておき、送信者がその都度決定するランク度に基づき、自動選択されるようにしてもよい。

【０１５６】

【発明の効果】

以上の説明で明らかなように、本発明によれば、ネットワーク通信における通信傍受等を未然に防いだ安全性の高い通信を簡易に実現可能となる。

【図面の簡単な説明】

【図１】

本発明に適用されるアドレス帳の内容の一例を示す図である。

【図２】

本発明に係る暗号化処理の内容の一例を概念的に示す図である。

【図３】

本発明に係る複合化処理の内容の一例を概念的に示す図である。

【図４】

電子メール送信時におけるＣＰＵの動作内容の全体を示すフローチャートである。

【図５】

自動暗号化処理の詳細内容を示すフローチャートである。

【図６】

電子メール受信後の復号化処理に係るＣＰＵの動作内容の詳細を示すフローチャートである。

【図７】

「配布」に係る取り決めの内容を示す図である。

【図８】

秘密鍵方式利用におけるアドレス帳の内容の一例を示す図である。

【図９】

秘密鍵方式利用における通信態様を模式的に示す図である。

【図１０】

公開鍵方式利用におけるアドレス帳の内容の一例を示す図である。

【図１１】

公開鍵方式利用における通信態様を模式的に示す図である。

【図１２】

暗号化方式および複合化方式登録の態様を説明するための図である。

【図１３】

多重暗号化に係るアドレス帳形式の一例を示す図である。

【図１４】

多重暗号化に係る処理内容（手順）を示す図である。

【図１５】

多重調整項目が追加されたアドレス帳の内容を示す図である。

【図１６】

多重暗号化における処理手順自動変更に係るアドレス帳の形式の一例を示す図である。

【図１７】

電話機暗号化通信に係る電話機のメモリ内容を示す図である。

【図１８】

電話機暗号化通信に係る文字列コード同士の関係を示す図である。

【図１９】

通常のネットワーク通信に係る問題点を説明するための図である。

【符号の説明】

1　送信元のコンピュータ端末機

2　送信先のコンピュータ端末機

（ａ）秋山氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
Ｘ社	Xcp@kabu‥‥	KCax	Cax	KPxa	Pxa
伊藤	Itou@asn‥‥	KCai	Cai	KPia	Pia
斉藤	Saitou@uu‥‥	KCas	Cas	KPsa	Psa
馬場	Baba@yy‥‥	KCab	Cab	KPba	Pba

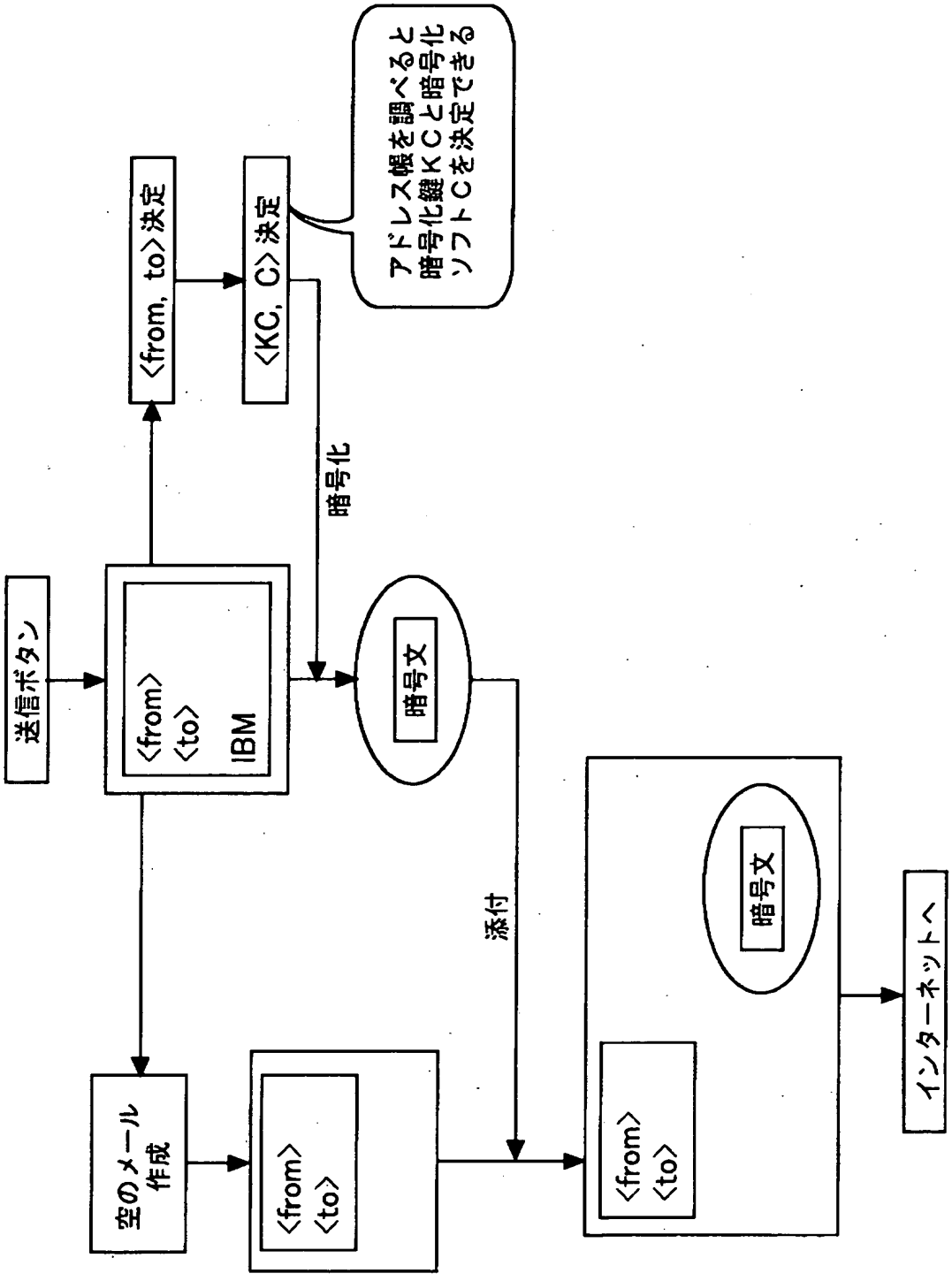
（ｂ）伊藤氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
Ｘ社	Xcp@kabu‥‥	KCix	Cix	KPxi	Pxi
秋山	Akiyama@ss‥‥	KCia	Cia	KPai	Pai
斉藤	Saitou@uu‥‥	KCis	Cis	KPsi	Psi
馬場	Baba@yy‥‥	KCib	Cib	KPbi	Pbi

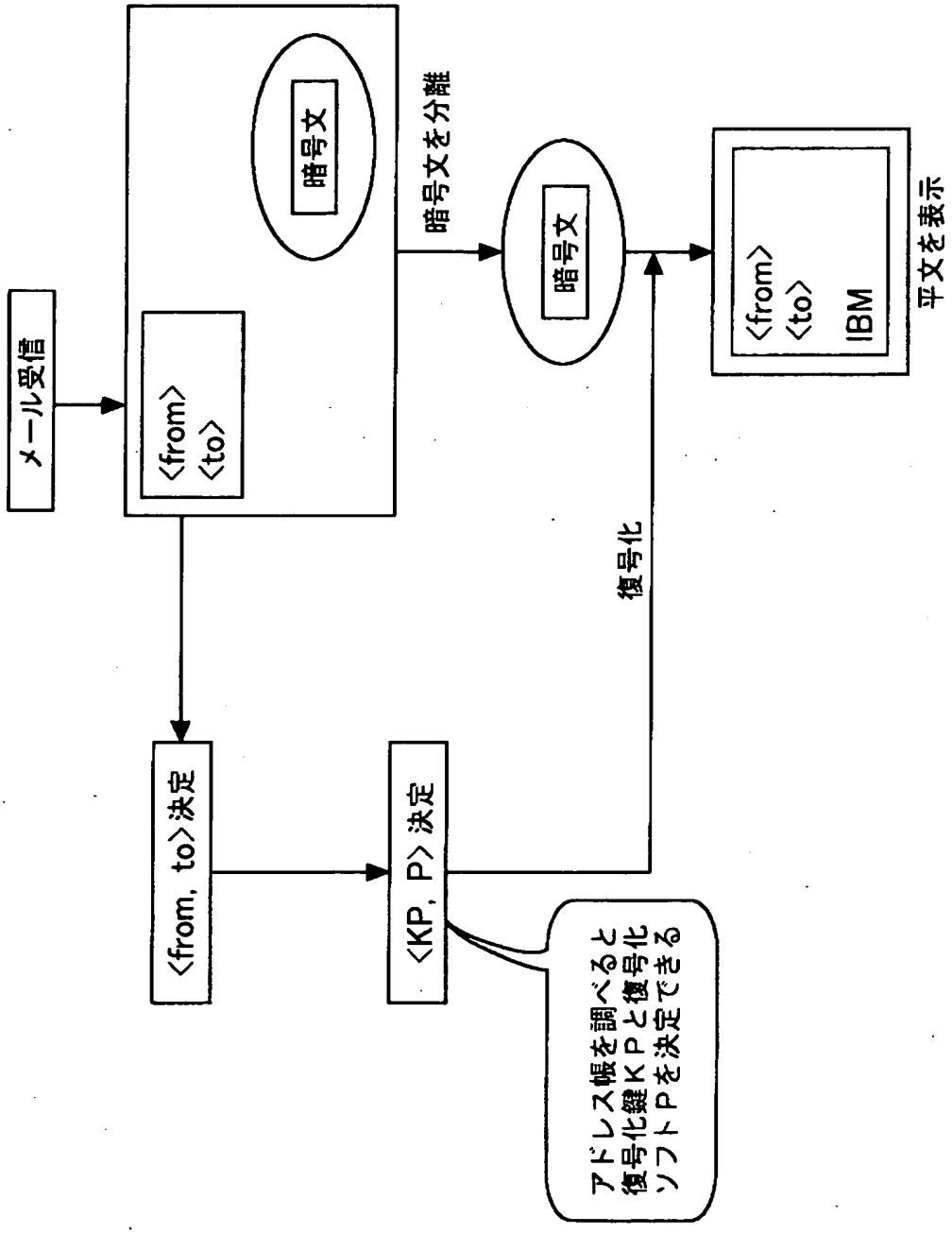
（ｃ）Ｘ社の顧客アドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
秋山	Akiyama@ss‥‥	KCxa	Cxa	KPax	Pax
伊藤	Itou@asn‥‥	KCxi	Cxi	KPix	Pix
遠藤	Endo@kk‥‥	KCxe	Cxe	KPex	Pex
山田	Yamada@yama‥	KCxy	Cxy	KPyx	Pyx

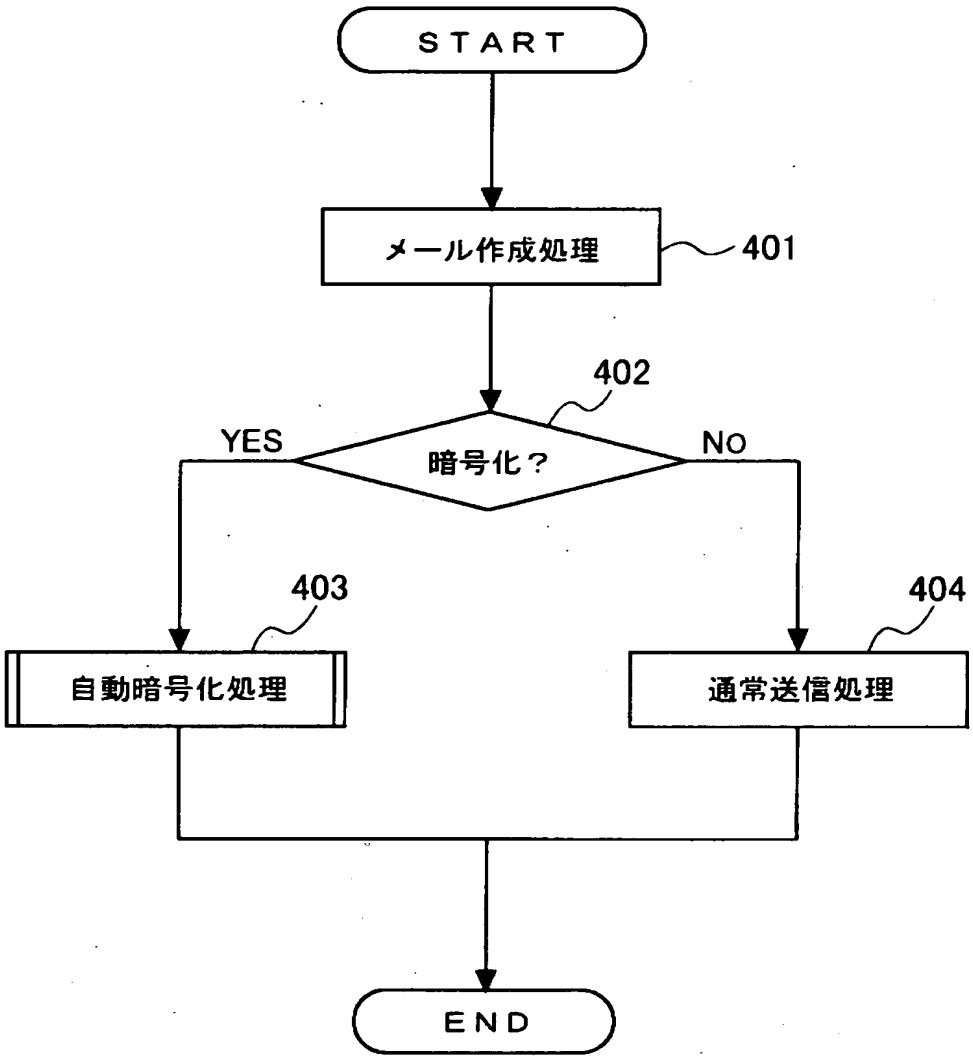
【図２】


送信ボタン
<from>
<to>
IBM
<from, to>決定
<KC, C>決定
アドレス帳を調べると
暗号化鍵ＫＣと暗号化
ソフトＣを決定できる
暗号化
暗号文
添付
空のメール
作成
<from>
<to>
<from>
<to>
暗号文
インターネットへ

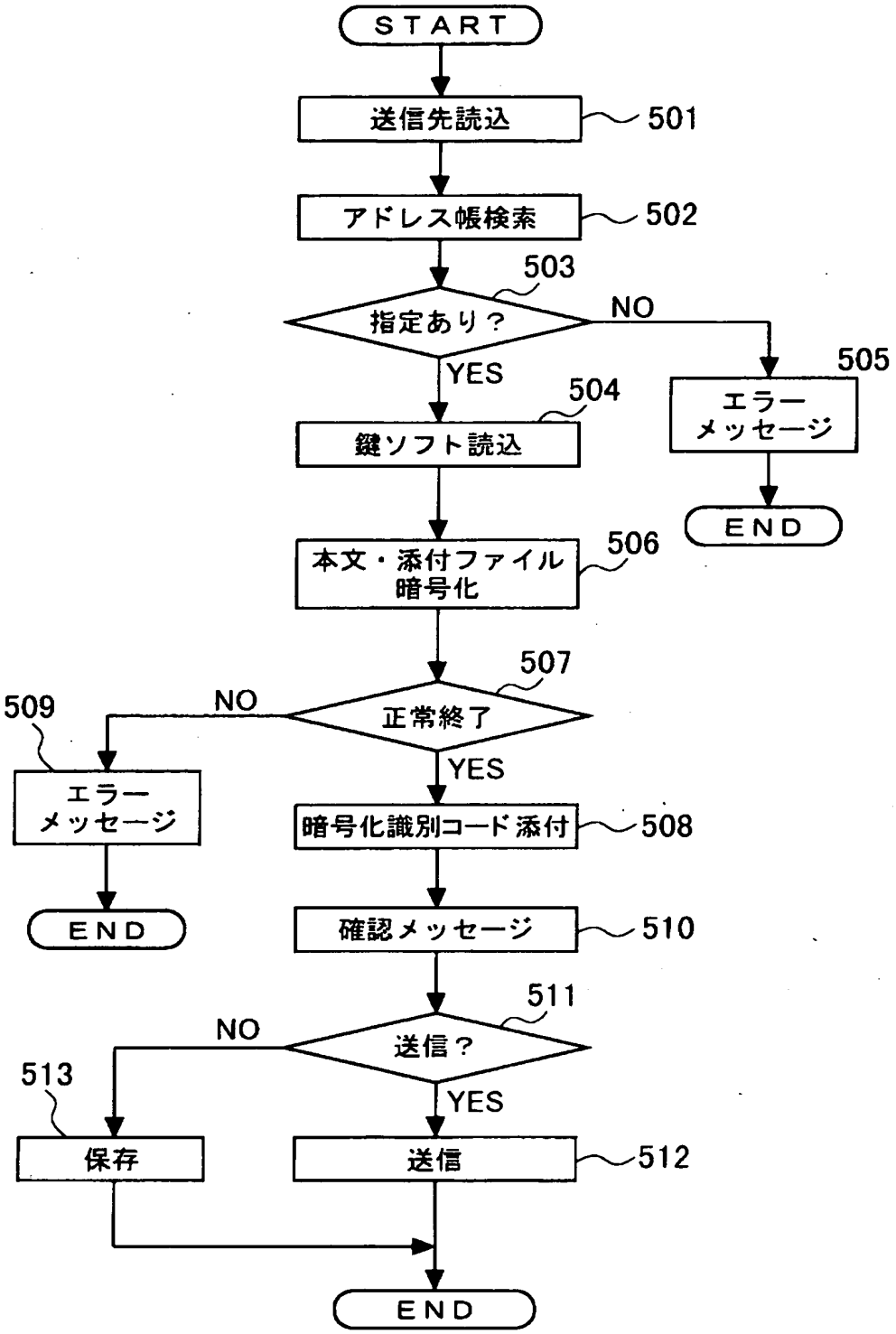
【図３】


メール受信
暗号文
<from>
<to>
暗号文を分離
暗号文
<from>
<to>
IBM
平文を表示
復号化
<from, to>決定
<KP, P>決定
アドレス帳を調べると
復号化鍵ＫＰと復号化
ソフトＰを決定できる

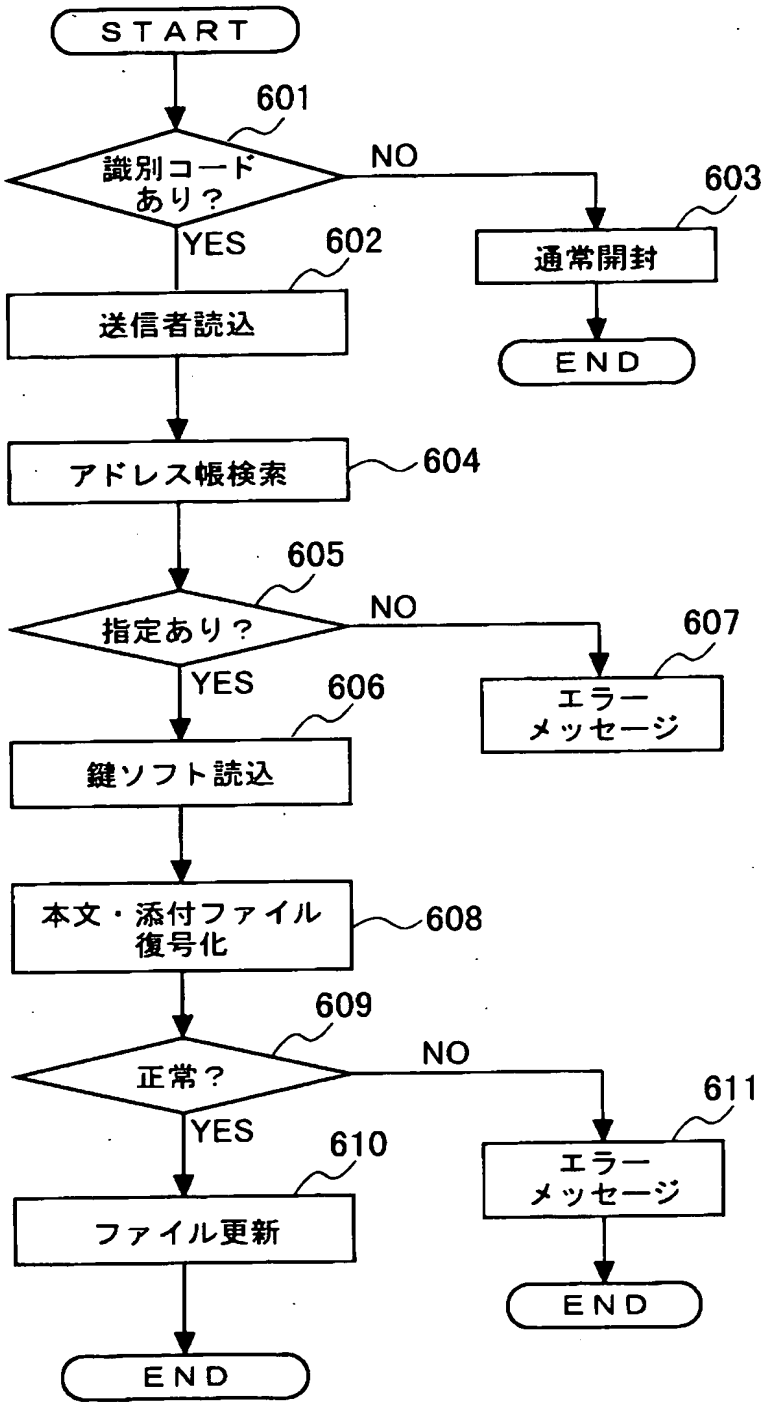
【図４】



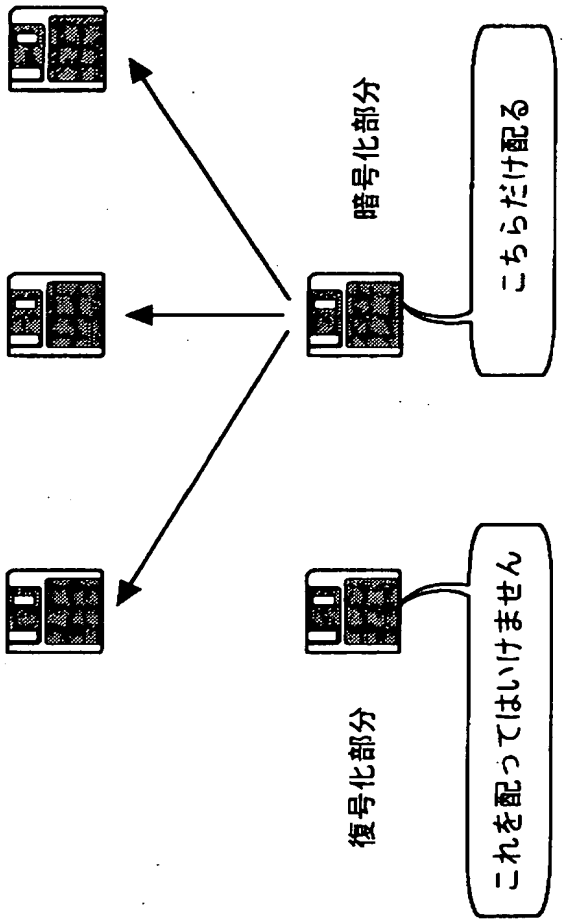
【図５】


START
送信先読込
501
アドレス帳検索
502
503
指定あり？
NO
YES
505
エラー
メッセージ
504
鍵ソフト読込
END
本文・添付ファイル
暗号化
506
507
509
NO
正常終了
YES
エラー
メッセージ
暗号化識別コード添付
508
END
確認メッセージ
510
511
NO
送信？
513
YES
保存
送信
512
END

【図６】


START
601
識別コード
あり？
NO
603
通常開封
YES
602
送信者読込
END
アドレス帳検索
604
605
指定あり？
NO
607
エラー
メッセージ
YES
606
鍵ソフト読込
本文・添付ファイル
復号化
608
609
正常？
NO
611
エラー
メッセージ
YES
610
ファイル更新
END
END

【図７】



【図８】

（ａ）秋山氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
Ｘ社	Xcp@kabu・・・・	KCax	Cax	25	P
伊藤	Itou@asn・・・・	KCai	Cai	1	P
斉藤	Saitou@uu・・・・	KCas	Cas	−2	P
馬場	Baba@yy・・・・	KCab	Cab	22	P

（ｂ）伊藤氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
Ｘ社	Xcp@kabu・・・・	KCix	Cix	KPxi	Pxi
秋山	Akiyama@ss・・・・	(−1)	C	KPai	Pai
斉藤	Saitou@uu・・・・	KCis	Cis	KPsi	Psi
馬場	Baba@yy・・・・	KCib	Cib	KPbi	Pbi

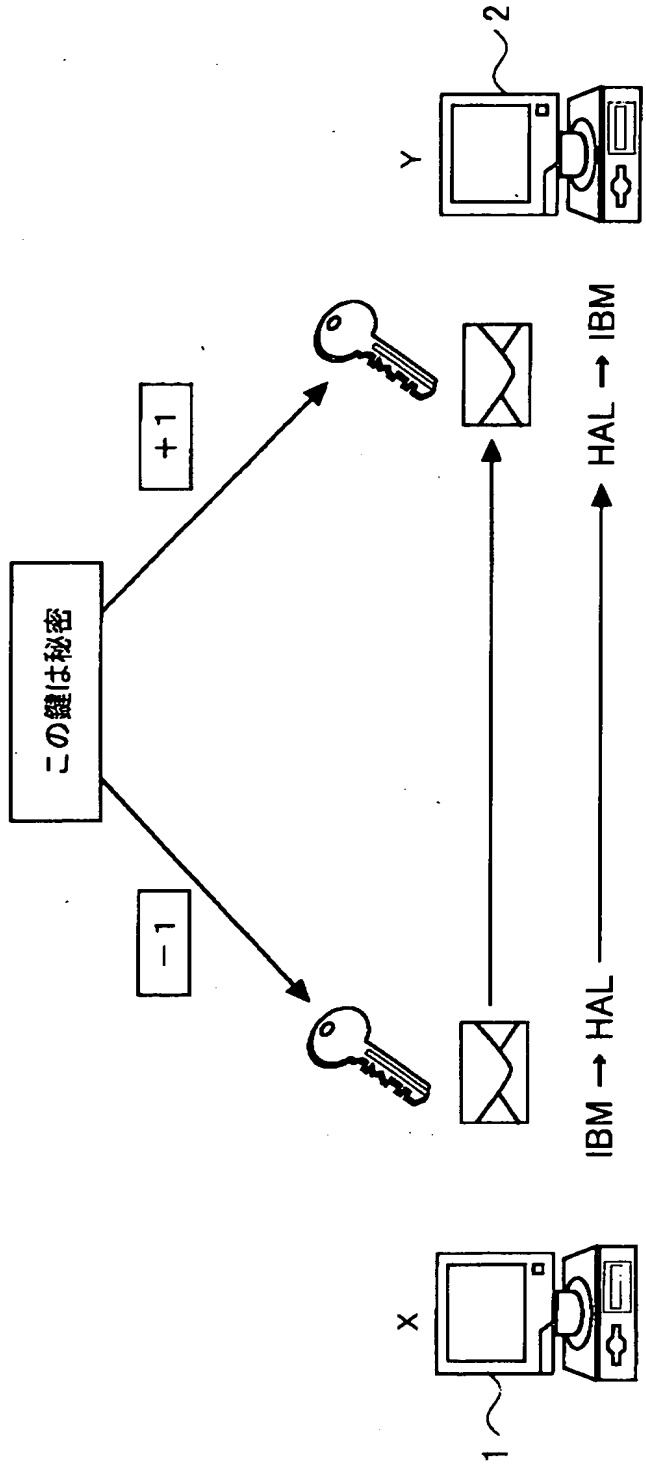
（ｃ）斉藤氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
Ｘ社	Xcp@kabu・・・・	KCsx	Csx	KPxs	Pxs
伊藤	Itou@asn・・・・	KCsi	Csii	KPis	Pis
秋山	Akiyama@ss・・・・	2	C	KPas	Pas
馬場	Baba@yy・・・・	KCsb	Csb	KPbs	Pbs

出証特２００１－３１１０４３８

特２００１－３２６９０８

【図９】



【図１０】

（ａ）秋山氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
Ｘ社	Xcp@kabu‥‥	KCax	Cax	d, n	PS
伊藤	Itou@asn‥‥	KCai	Cai	d, n	PS
斉藤	Saitou@uu‥‥	KCas	Cas	d, n	PS
馬場	Baba@yy‥‥	KCab	Cab	d, n	PS

（ｂ）伊藤氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
Ｘ社	Xcp@kabu‥‥	KCix	Cix	KPxi	Pxi
秋山	Akiyama@ss‥‥	e, n	C	KPai	Pai
斉藤	Saitou@uu‥‥	KCis	Cis	KPsi	Psi
馬場	Baba@yy‥‥	KCib	Cib	KPbi	Pbi

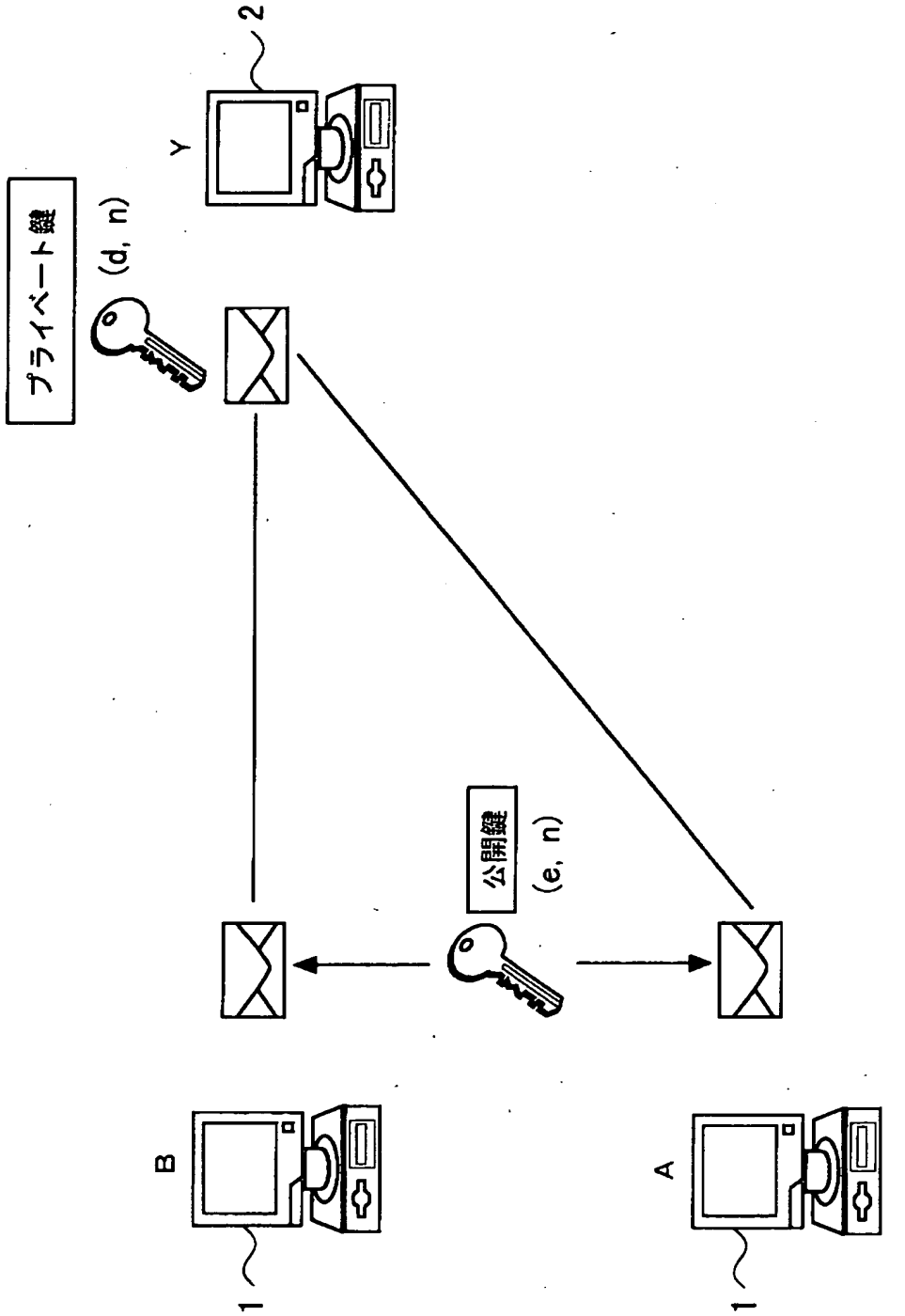
（ｃ）斉藤氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
Ｘ社	Xcp@kabu‥‥	KCsx	Csx	KPxs	Pxs
伊藤	Itou@asn‥‥	KCsI	CsI	KPis	Pis
秋山	Akiyama@ss‥‥	e, n	C	KPas	Pas
馬場	Baba@yy‥‥	KCsb	Csb	KPbs	Pbs

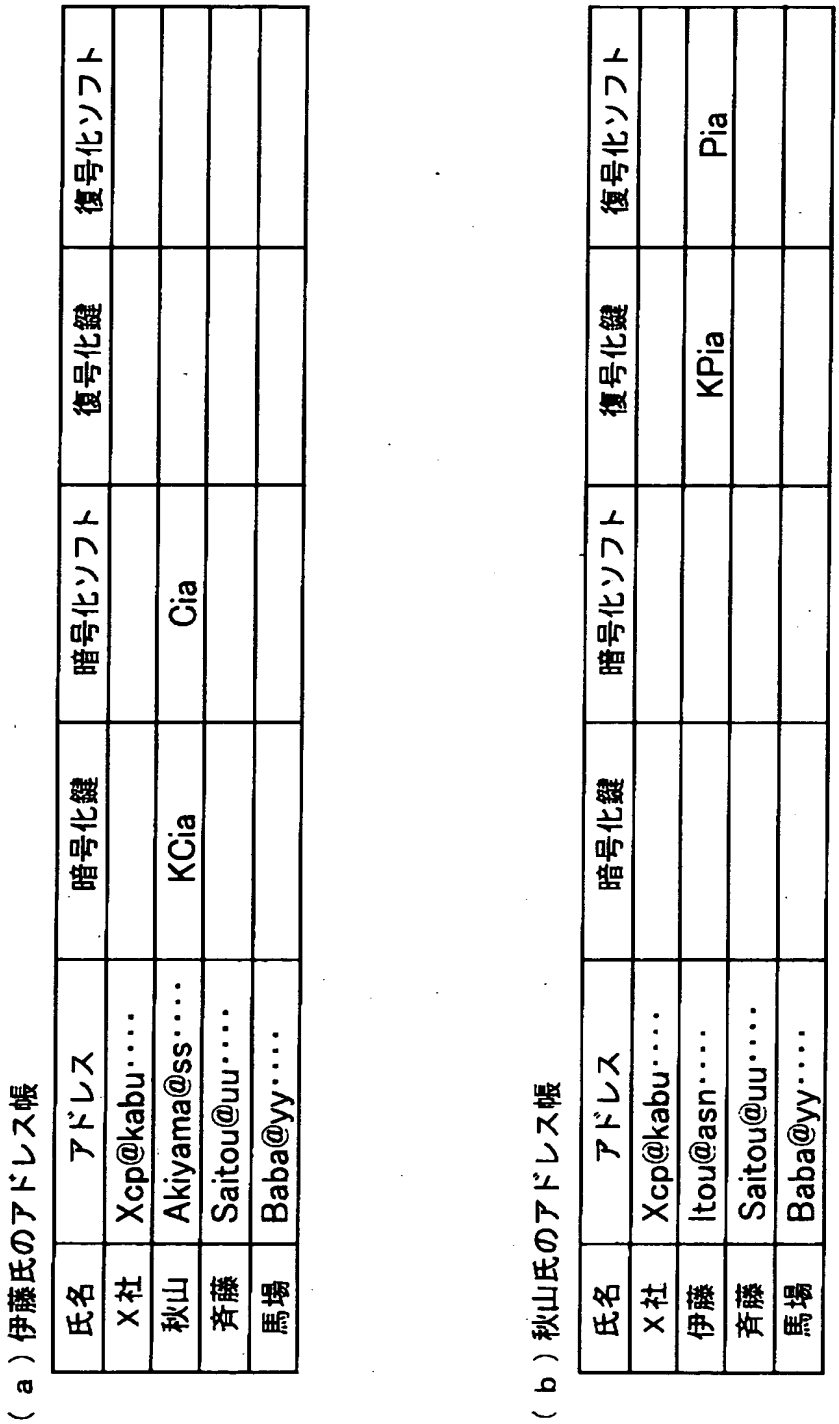
出証特２００１－３１１０４３８

特２００１－３２６９０８

【図１１】



【図１２】



（ａ）伊藤氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu・・・・				
秋山	Akiyama@ss・・・・	KCia	Cia		
斉藤	Saitou@uu・・・・				
馬場	Baba@yy・・・・				

（ｂ）秋山氏のアドレス帳

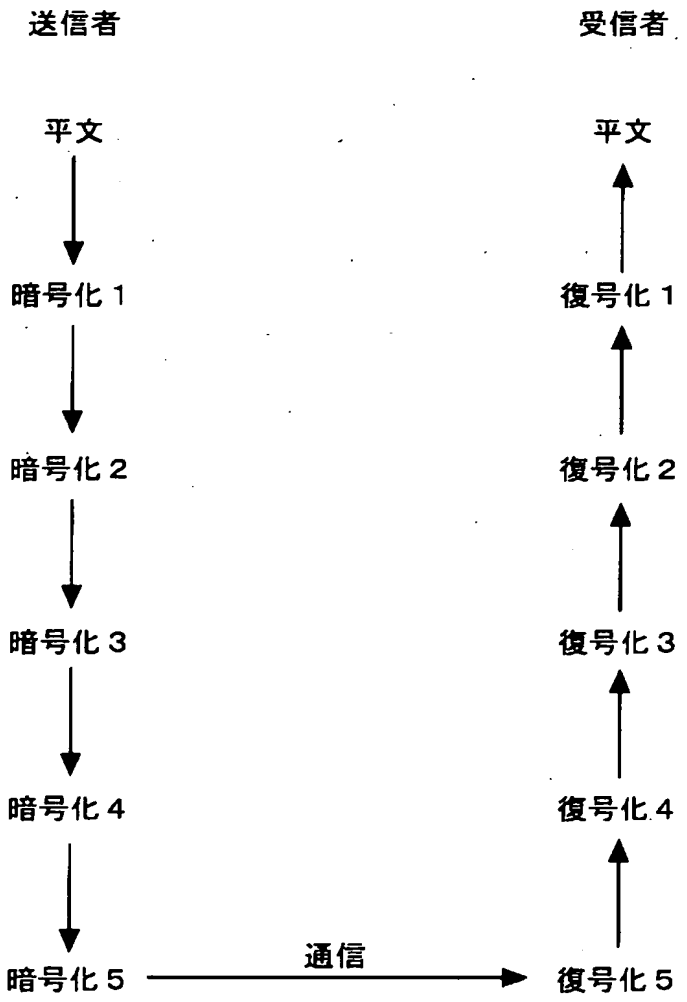
氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu・・・・				
伊藤	Itou@asn・・・・			KPia	Pia
斉藤	Saitou@uu・・・・				
馬場	Baba@yy・・・・				

【図１３】

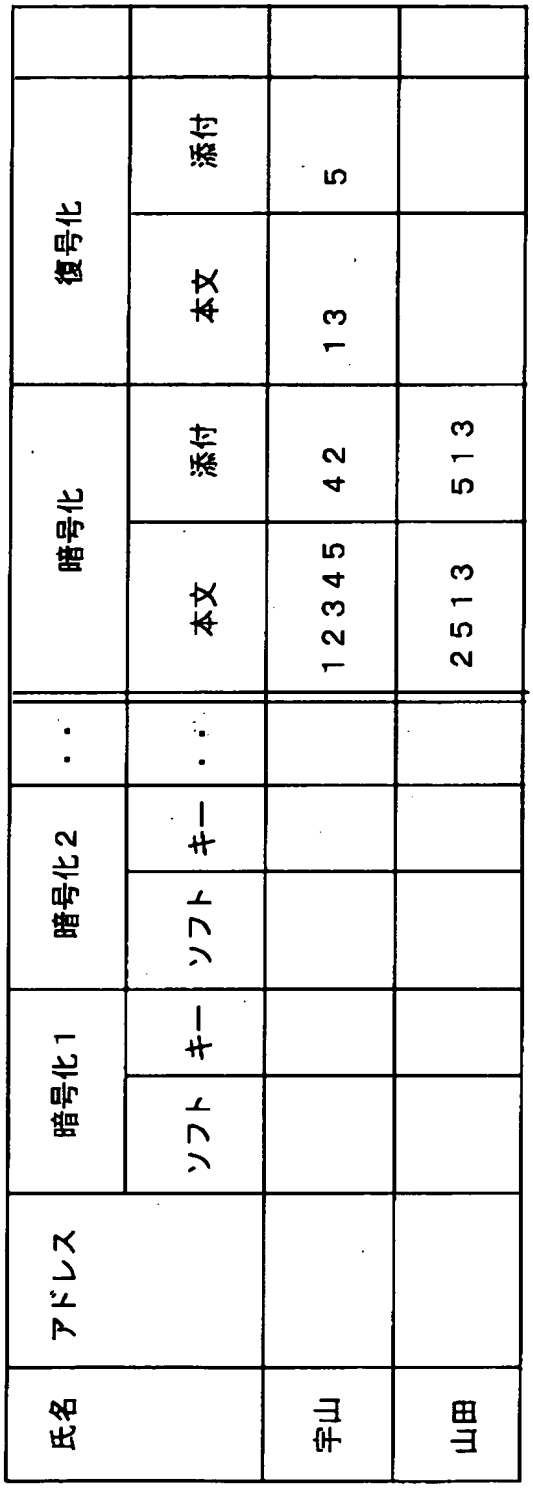
氏名	アドレス	暗号化１		暗号化２		・・・・・	復号化１		復号化２		・・・・・
		ソフト	キー	ソフト	キー	・・・・・	ソフト	キー	ソフト	キー	・・・・・
宇山											
山田											

【図１４】

例：５段の場合


送信者
受信者
平文
暗号化１
暗号化２
暗号化３
暗号化４
暗号化５
通信
平文
復号化１
復号化２
復号化３
復号化４
復号化５

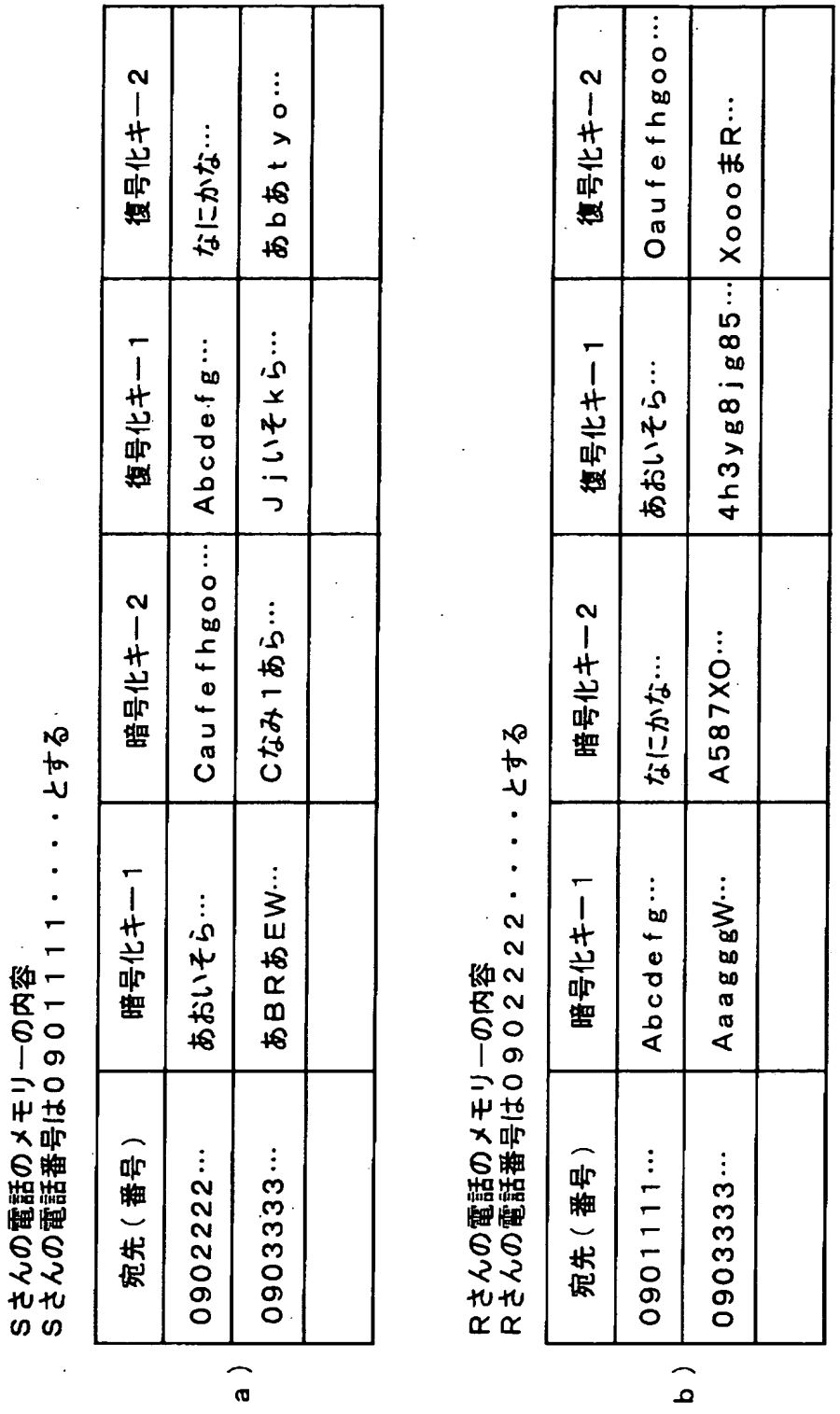
【図１５】


氏名
アドレス
暗号化1
ソフト
キー
暗号化2
ソフト
キー
・・
暗号化
本文
添付
復号化
本文
添付
宇山
山田
１２３４５
２５１３
４２
５１３
１３
５
・・

【図１６】

氏名	アドレス	暗号化１		暗号化２		……	暗号化		１月ごとの置換（スケジュールファイルの内容）	
		ソフト	キー	ソフト	キー	……	本文	添付	本文	添付
宇山							１２３４５	４２	１２３４５ ３１５２４ ……	４２ ２４
山田							２５１３	５１３	２５１３ ５３２１ ……	５１３ ３５１

【図１７】



Ｓさんの電話のメモリーの内容
Ｓさんの電話番号は０９０１１１１・・・・とする

（ａ）

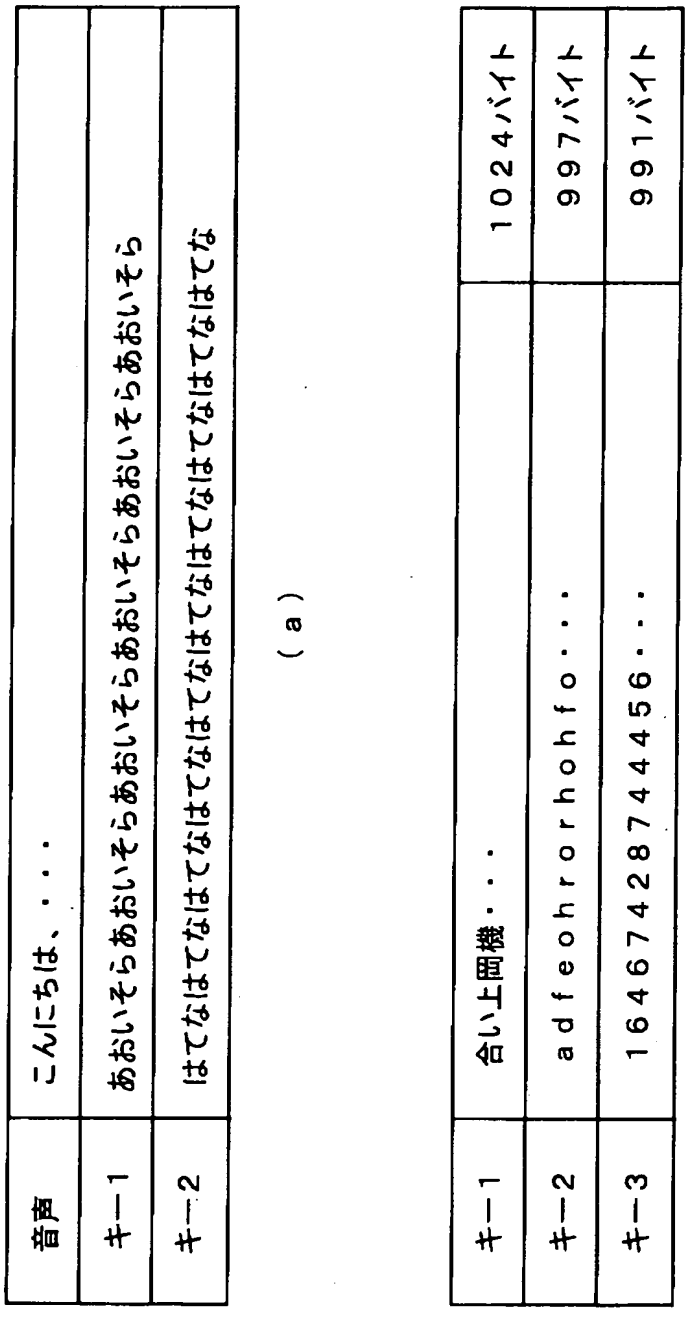
宛先（番号）	暗号化キー１	暗号化キー２	復号化キー１	復号化キー２
0902222…	あおいそら…	Caufefhgoo…	Abcdefg…	なにかな…
0903333…	あBRあEW…	Cなみ１あら…	Ｊｊいそｋら…	あｂあｔｙｏ…

Ｒさんの電話のメモリーの内容
Ｒさんの電話番号は０９０２２２２・・・・とする

（ｂ）

宛先（番号）	暗号化キー１	暗号化キー２	復号化キー１	復号化キー２
0901111…	Abcdefg…	なにかな…	あおいそら…	Oaufefhgoo…
0903333…	AaagggW…	A587XO…	4h3yg8jg85…	XoooまR…

【図１８】



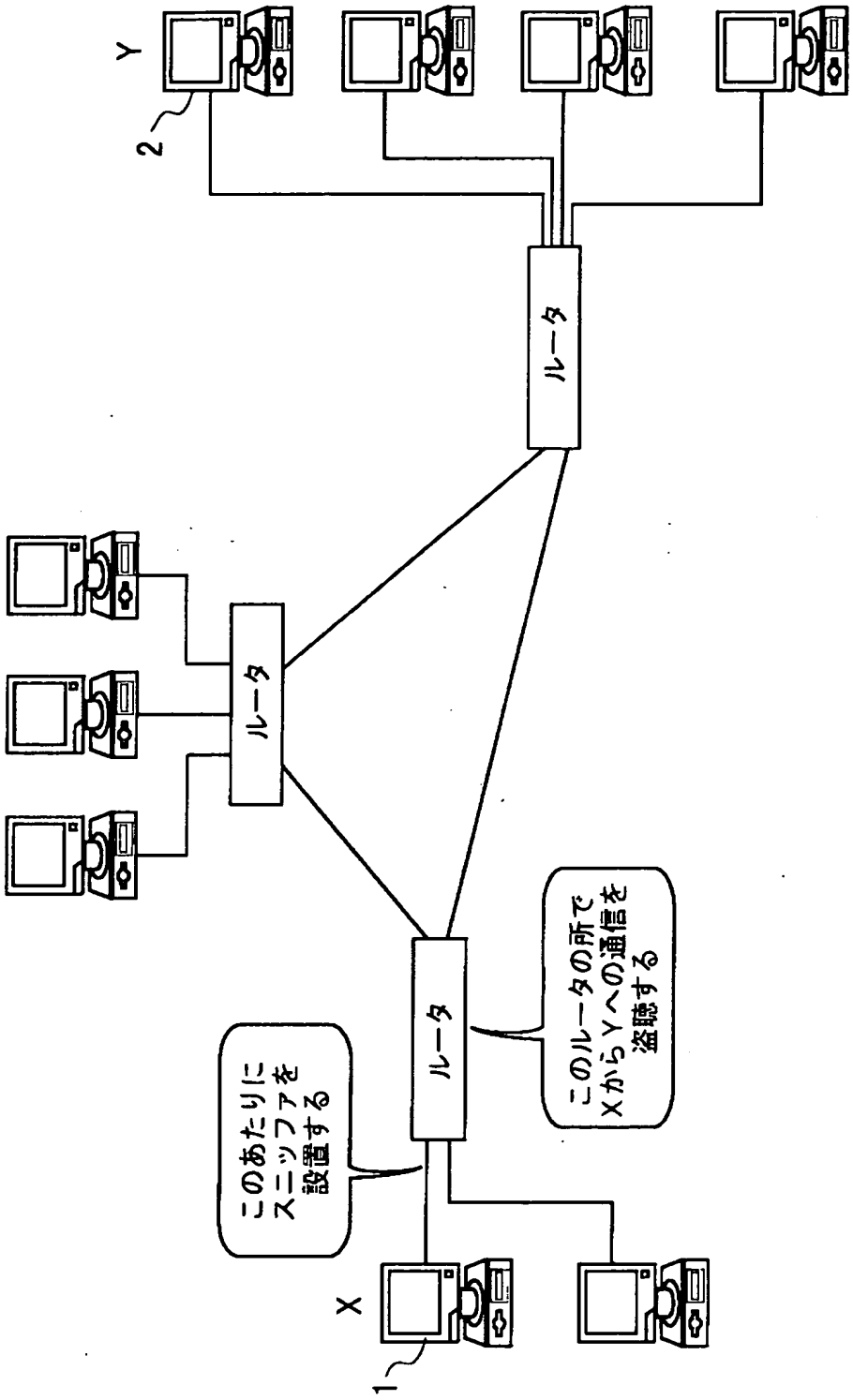
音声	こんにちは、・・・
キー１	あおいそらあおいそらあおいそらあおいそらあおいそらあおいそら
キー２	はてなはてなはてなはてなはてなはてなはてなはてなはてなはてな

（ａ）

キー１	合い上囲機・・・	１０２４バイト
キー２	ａｄｆｅｏｈｒｏｒｈｏｈｆｏ・・・	９９７バイト
キー３	１６４６７４２８７４４４５６・・・	９９１バイト

（ｂ）

【図１９】


Y
2
ルータ
ルータ
ルータ
このルータの所で
XからYへの通信を
盗聴する
このあたりに
スニッファを
設置する
X
1

【書類名】　　要約書

【要約】

【課題】　より安全で信頼性のあるネットワーク通信を実現するための秘密通信方法を提供する。

【解決手段】　記憶装置と演算装置を利用できる情報機器による暗号を利用した秘密通信において、送信者と受信者の順序対に対して一意的に決まる暗号化方式と復号化方式に従ってデータの暗号化または復号化を自動的に行い、かつ、順序対に対応する暗号化方式を受信者が前もって自由に指定しておくことができるようにする。

【選択図】　　図２

認定・付加情報

特許出願の番号	特願２００１－３２６９０８
受付番号	５０１０１５７１９１９
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１３年１２月　４日

＜認定情報・付加情報＞

【提出日】　平成13年10月24日

次頁無

出願人履歴情報

識別番号　〔３００００８５８６４〕

１．変更年月日　２０００年１１月１８日
［変更理由］　新規登録
住　所　神奈川県横須賀市久里浜８－３０－１５－５０４
氏　名　宇山　靖政